

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>					
1. REPORT DATE (DD-MM-YYYY) 07-06-2011		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) 24 July 2010-7 June 2011	
4. TITLE AND SUBTITLE CYBER AS A "TEAM SPORT": OPERATIONALIZING A WHOLE-OF-GOVERNMENT APPROACH TO CYBERSPACE OPERATIONS J201, 14				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Elizabeth A. Myers, Civ, Department of Defense				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) National Defense University, Joint Forces Staff College, Joint Advanced Warfighting School (JAWS) 7800 Hampton Blvd Norfolk, VA 23511				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for Public Release, Distribution is Unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT Cyberspace and its associated operations present both opportunities and challenges for military and United States Government decision-makers and planners. Cyberspace is man-made, dynamic, and intrinsically linked to not only Department of Defense (DoD) capabilities across the other four domains, but to national, commercial and global capabilities and interests as well. The implications for cyberspace, its defense and freedom of operations within, extend well beyond DoD's, and even the U.S. Government's, span of control and influence. In order to effectively navigate the complexities posed by cyberspace and ensure that the United States gains and maintains strategic advantage in the future battlefield using cyberspace operations, a whole-of-government approach is required. This thesis examines the current strategic guidance, organizational framework, governance and responsibilities associated with cyberspace operations. It identifies the issues and challenges currently facing the U.S. in operationalizing a whole-of-government approach to defending and operating in the cyberspace domain. Finally, this paper presents recommendations for improvements in the implementation and operationalization of a whole-of-government approach to cyberspace operations.					
15. SUBJECT TERMS Cyber, cyberspace, cyberspace operations, whole-of-government, computer network operations					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU-Unclassified	18. NUMBER OF PAGES 120	19a. NAME OF RESPONSIBLE PERSON
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (Include area code) 757-443-6301

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL



**CYBER AS A “TEAM SPORT”: OPERATIONALIZING A WHOLE-OF-
GOVERNMENT APPROACH TO CYBERSPACE OPERATIONS**

by

Elizabeth A. Myers

Department of Defense

**CYBER AS A "TEAM SPORT": OPERATIONALIZING A WHOLE-OF-
GOVERNMENT APPROACH TO CYBERSPACE OPERATIONS**

by

Elizabeth A. Myers

Civilian, Department of Defense

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Signature: 

27 April 2011

Thesis Adviser:


Signature: 

J. Bruce Miller, Col, USMC

Approved by:

Signature: 

**Charles Cunningham, Lt Gen (Ret), USAF
Committee Member**

Signature: 

**Carmine Cicalese, COL, USA
Committee Member**

Signature: 

**Joanne M. Fish, CAPT, USN, Director,
Joint Advanced Warfighting School**

ABSTRACT

Cyberspace and its associated operations present both opportunities and challenges for military and United States Government decision-makers and planners. The Pentagon has formally recognized cyberspace as a domain of warfare. Cyberspace is man-made, dynamic, and intrinsically linked to not only Department of Defense (DoD) capabilities across the other four domains, but also to national, commercial and global capabilities and interests as well. The implications for cyberspace, its defense and freedom of operations within, extend well beyond DoD's, and even the U.S. Government's, span of control and influence. Increasingly, foreign influence and threats are shaping the cyber battlefield. In order to effectively navigate the complexities posed by cyberspace and ensure that the United States gains and maintains strategic advantage in the future battlefield using cyberspace operations, a whole-of-government approach is required. The United States will need to leverage the unique capabilities of the various actors across the diplomatic, information, military, economic, financial, intelligence, and law enforcement (DIMEFIL) spectrum to successfully defend against the asymmetric threats posed in cyberspace while ensuring freedom of action within the domain. This thesis examines the current strategic guidance, organizational framework, governance and responsibilities associated with cyberspace operations. It identifies the issues and challenges currently facing the U.S. in operationalizing a whole-of-government approach to defending and operating in the cyberspace domain. Finally, this paper presents recommendations for improvements in the implementation and operationalization of a whole-of-government approach to cyberspace operations.

ACKNOWLEDGEMENT

Many people deserve my thanks and gratitude for their guidance and assistance in completing this thesis. Over the past several years, I have been fortunate to work with and learn about cyberspace operations from a number of individuals at U.S. Cyber Command (and its predecessor organizations) and the National Security Agency. It is the collective knowledge I gained from those colleagues on the issues, requirements and challenges facing DoD and U.S. Government cyber operations and future capabilities which led me to pursue this thesis.

I would like to thank my JAWS faculty and thesis advisor, Colonel Bruce Miller, USMC, for his encouragement, guidance and support throughout the course of this project. The staff at the JFSC's Ike Skelton Library was outstanding in providing research assistance, finding obscure reference materials and ensuring the final document followed all the appropriate citation standards. A particular thanks to Dawn Joines and Jason Girard for their assistance. Thank-you as well to Dr. Phil Sauer, DoD civilian and University of Maryland professor, and Dr. Steven Poole, Oak Ridge National Laboratory, for their outside review and comments on the paper and for providing me with their expert insights on cyberspace issues.

A special thank-you to my colleagues in JAWS Seminar 3—first, thank-you for your service and sacrifice to our country; and second, a heartfelt thanks for your wisdom, assistance, forbearance, humor and most of all, friendship, which have made this, and our other tasks and assignments over the course of the year, a bearable and learning experience! I will miss you all.

Finally, and most importantly, I would like to thank my family for their love and support, especially my husband. Thank-you for putting up with a “geo-bachelor” separation for nearly a year (including missing our 25th wedding anniversary), and providing loving encouragement and support throughout—I love you!

TABLE OF CONTENTS

INTRODUCTION	1
CHAPTER 1: A NEW FRONTIER: UNDERSTANDING THE DOMAIN	6
CHAPTER 2: STRATEGIC DIRECTION AND KEY PLAYERS	28
CHAPTER 3: ISSUES AND CHALLENGES	46
CHAPTER 4: RECOMMENDATIONS.....	61
CHAPTER 5: CONCLUSION	73
APPENDIX 1: OBAMA ADMINISTRATION’S CYBERSPACE POLICY REVIEW RECOMMENDATIONS	77
APPENDIX 2: KEY ORGANIZATIONS ENGAGED IN CYBERSPACE OPERATIONS.....	80
APPENDIX 3: FINDINGS FROM CYBER STORM I (2006) AND II (2008).....	92
GLOSSARY	95
BIBLIOGRAPHY	98

INTRODUCTION

“...Cyber (is) a team sport; successful defense in any one part depends on the shared efforts of agencies, industry, allies and mission partners who watch their own networks for problems that could affect them all.”¹

The United States military is building its capabilities to operate and defend in the newest war-fighting domain: cyberspace. To that end, the military is armed with a new command and is developing doctrine and plans, building defensive and offensive weapons systems, and recruiting and training a workforce to secure our capabilities, address threats and ensure freedom of maneuver in cyberspace. The cyberspace domain, however, is one where the U.S. military cannot assume superiority: first, the domain is already contested as there are a growing number of foreign actors (both state and non-state) developing and attacking U.S. systems using sophisticated capabilities; and second, U.S. military capabilities alone cannot secure the expanse of the domain given the inter-dependent (and borderless) nature of the domain with government and commercial users and providers worldwide (including those which provide the capabilities and capacity for the military to operate). While cyberspace and its associated technologies provide the military with many advantages in which to operate across all war-fighting domains, a heavy reliance on its capabilities makes military systems increasingly vulnerable to foreign threats and actions, as well as to inherent weaknesses within the technology.

How then can the U.S. military ensure success (secure defense of military and critical U.S. Government (USG) networks/infrastructure while enabling freedom of

¹ General Keith B. Alexander, Commander United States Cyber Command, speaking on the Cyber Command Posture Statement, on 23 September 2010, before the House Committee on Armed Services, 111th Cong., 2nd sess., 9.

maneuver or operations) in the cyberspace domain? In order to navigate effectively the complexities posed by cyberspace and ensure that the United States gains and maintains strategic advantage in the future cyberspace battlefield, a whole-of-government, and arguably, a whole-of-nation, approach is required. The United States will need to leverage the unique capabilities of the various actors across the diplomatic, information, military, economic, financial, intelligence, and law enforcement (DIMEFIL) spectrum to successfully defend against the asymmetric threats posed in cyberspace. Each USG department and agency, each military service component, and each foreign and industry partner, bring complementary cyber capabilities to the combined fight in the cyberspace domain. This thesis will explore the issues and challenges facing the USG and pose recommendations to operationalize a whole-of-government approach to cyberspace operations. A whole-of-government approach will enhance military operations and ensure superiority in the cyberspace domain.

Cyberspace and its associated operations present both opportunities and challenges for military and government decision-makers and planners. The Pentagon has formally recognized cyberspace as a domain of warfare. Cyberspace is man-made, dynamic, and intrinsically linked to not only Department of Defense (DoD) capabilities across the other four domains (land, sea, air and space), but to national, commercial and global capabilities and interests as well. The 2010 *Quadrennial Defense Review* (QDR) acknowledges that the interdependence of cyberspace means DoD networks are heavily dependent on commercial infrastructure.² The implications for cyberspace, its defense and freedom of operations within, extend well beyond DoD's span of control and

² *Quadrennial Defense Review, 2010*, (Washington, DC: Department of Defense, 2010), 39.

influence. Securing the networks and ensuring freedom of action in cyberspace are national security issues, with implications for all elements of national power.

In response to greater interdependencies of and growing threats to the cyberspace domain, the USG and military are investing heavily in capabilities to defend, secure and operate in cyberspace. While cyberspace and the need for its defense is not a new concept, there have been a number of new strategic, doctrinal and organizational changes implemented (or in the process of being implemented) since 2009 focused on the imperative for USG and DoD action related to cyberspace. The need to address cyber security and protect the United States' ability to act freely in cyberspace is called out in the Obama Administration's May 2010 *National Security Strategy* (NSS). In the NSS, cyberspace is identified as a "strategic national asset, and protecting it...a national security priority."³ A new sub-unified command, U.S. Cyber Command, formally stood up in May 2010, and is responsible for "full-spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./Allied freedom of action in cyberspace and deny the same to our adversaries."⁴ The Pentagon is preparing a new strategy, scheduled for release in early-mid 2011, which will address the military's active defense of the cyberspace domain. As the military incorporates cyber-related components into existing and future plans, military commanders and planners at all levels, as well as inter-agency partners, will need to understand the inter-dependencies of the domain and how to apply effectively a whole-of-government approach across the DIMEFIL spectrum to meet national and military objectives successfully. Recent military publications go as far as to

³ *National Security Strategy*, (Washington, DC: U.S. President, 2010), 27.

⁴ U.S. Strategic Command Website, "U.S. Cyber Command Mission Statement," U.S. Strategic Command, <http://www.stratcom.mil/factsheets/cc/> [accessed 5 January 2011].

project that the United States' ability to maneuver freely in cyberspace amplifies all instruments of national power and that ability, in and of itself, is an emerging instrument of power.⁵

Most policymakers, military officials and industry security experts agree that the best approach to maintaining strategic advantage for the United States in cyberspace is to work in partnership across defense and government agencies and departments, and in coordination with the commercial sector and with our allies. There are a number of issues which stand in the way of the United States being able to realize and optimize the country's capabilities to secure our national interests in cyberspace. These issues range from achieving a common definition and understanding as to what is meant by cyberspace to more complex issues related to roles, responsibilities and legal authorities. ADM (Ret) John M. (Mike) McConnell, former Director of National Intelligence and former Director, National Security Agency (NSA), has asserted that key to protecting our strategic assets is the creation of an integrated solution: "NSA is allowed to exploit, DoD is in charge of attack, DHS is in charge of protecting the nation, but, in cyber, these activities are very closely related."⁶ Without resolving the issues which stand in the way of creating an integrated USG approach to defending and operating in cyberspace, military and government capabilities to defend and operate within the domain will remain limited, potentially putting U.S. security at risk.

⁵ United States Joint Forces Command, *The Joint Operating Environment 2010*, (Suffolk, VA: Joint Forces Command, 2010), 34.

⁶ "Cyber is Major Symposium Subject," *Spacewatch*, May 2010 Vol 9, no. 5, <http://newsletters.spacefoundation.org/spacewatch/articles/id/470> (Accessed on 13 January 2011).

The first chapter of this thesis addresses the major core issues associated with understanding the cyberspace domain: how cyberspace and related activities are defined, characteristics which make the cyberspace domain different from the other war-fighting domains, and the current threat environment facing cyberspace operations. The second chapter explores the guiding documents, roles and responsibilities of principal USG departments, agencies, and partner organizations in defending and operating in cyberspace. The third chapter then reviews the challenges and issues which USG departments and agencies face in operationalizing a whole-of-government approach to conducting cyberspace operations. Chapter four outlines recommendations which, if implemented, will serve to establish a coherent and operationally sound whole-of-government approach to addressing the strategic challenges and opportunities presented by cyberspace operations.

Limitations

A caveat on the development of this thesis: the majority of current policy and doctrine related to offensive computer network operations and to some extent, defensive vulnerabilities, across the U.S. Government resides within the classified realm. Therefore, specifics related to offensive operations will not be discussed in this paper. This thesis is based on information from unclassified and open sources. Additionally, U.S. Government actions and positions related to cyberspace operations and cybersecurity are rapidly evolving and there is a plethora of updates and new information, sometimes on a near daily basis. The information cut-off for this thesis is roughly 1 April 2011.

CHAPTER 1: A NEW FRONTIER: UNDERSTANDING THE DOMAIN

“Cyberspace, like outer space, is a lawless domain, without rules and no boundaries, it happens with the speed of light.” CJCS, ADM Michael Mullen¹

Virtually all aspects of our society today, whether private, commercial or government, rely on capabilities resident in, or provided by, the cyberspace domain. This includes the critical infrastructures governing power, telecommunications, finance and transportation sectors, healthcare and emergency response capabilities, as well as individuals’ ability to access the Internet, use automated teller systems/banking, or even view television. For the military, many, if not most, of its weapons systems, command and control, intelligence and logistics capabilities in the land, air, sea and space domains leverage or ride to some extent, on infrastructure provided by information/cyber technologies. The ability to fight in and through the cyber domain requires freedom of secure access and movement in the domain. In order to defend and operate effectively in the cyber domain, it is important to understand the domain, the characteristics that distinguish the domain, and the threats facing operations within the domain.

Why Definitions Matter

*“Cyberspace is a defensible domain. We should study cyberspace in the same way we study the other domains, to understand how the principles of the military art apply there.”*²

One of the most difficult challenges facing the U.S. Government in instituting a comprehensive approach which ensures successful cyberspace operations is to adopt a

¹ “Adm. Mike Mullen: China Not the Only Cyber Threat,” *The New NewInternet*, <http://www.thenewnewinternet.com/2011/01/14/adm-mike-mullen-china-not-the-only-cyber-threat/> (accessed on 6 March 2011).

² General Keith B. Alexander, Commander United States Cyber Command, speaking on the Cyber Command Posture Statement, on 23 September 2010, before the House Committee on Armed Services, 111th Cong., 2nd sess.

common definition and understanding as to what constitutes the “cyberspace domain.”³

What follows in this section is a discussion of how some of those definitions have distinct implications for the actions of various USG agencies and departments.

Defense officials acknowledge that one of the key steps toward achieving an effective USG approach to cyberspace security and operations is to establish a common lexicon, which includes standardized taxonomy and terminology associated with cyber, cyber attacks and cyber war. Officials in the Intelligence, Defense and Energy communities, interviewed by the author, indicate that the lack of a common definition for what constitutes the cyberspace domain inhibits cross-agency action and cooperation. An unidentified U.S. official quoted in a recent Washington Post article noted that defining the cyber battlefield is critical to operating within and defending it successfully.

According to the unnamed official in the article, “operations in the cyber-world can’t be likened to Yorktown, Iwo Jima or the Inchon landing....defining the battlefield too broadly could lead to undesired consequences.”⁴

Understanding what the domain is (and is not) enables government, defense, homeland, and law enforcement agencies, as well as the private sector/industry to better understand what it means to operate in cyberspace, helps define roles and missions, clarifies authorities, synchronizes actions and manages risk. Without reaching an international consensus on a definition, it will be difficult to establish international legal statutes related to cyber warfare or the conduct of operations within, and the defense of, cyberspace. The USG adheres to strict laws and rules of engagement, which is not

³ The Glossary at the end of this document lists accepted DoD definitions of commonly used cyber-related terms.

⁴ Ellen Nakashima, “Pentagon is Debating Cyber-Attacks,” Washington Post, November 6, 2010, 7.

necessarily true of other actors operating in cyberspace.

Franklin Kramer, national security expert and Distinguished Research Fellow at the Center for Technology and National Security Policy of the National Defense University (NDU), in Congressional testimony, noted that cyber can be defined in many ways, and the variety of definitions should be used to aid policy and analysis, not place limitations upon them.⁵ According to Kramer, cyber extends beyond the Internet and span of related computer technologies, and must take into consideration the human dimension (i.e., the impact of social media on the recent unrest in the Middle East), military net-centric operations, the influences of electronic media and cell phones and associated interfaces and applications.⁶

The term “cyberspace” was initially used by William Gibson in his 1984 science fiction novel, *Neuromancer*. Gibson defined cyberspace as a “graphic representation of data abstracted from the banks of every computer in the human system of ...unthinkable complexity....”⁷ In common usage, the term has generally evolved to “the online world of computer networks and the Internet.”⁸ Richard A. Clarke, former Special Advisor to the President on Cybersecurity and Cyberterrorism in the George W. Bush Administration, defined cyberspace in his recent book, *Cyber War*, as:

⁵ House Armed Services Committee, “Statement of Franklin D. Kramer before the House Armed Services Committee Subcommittee on Terrorism and Unconventional Threats, 1 April 2008,” http://www.carlisle.army.mil/DIME/documents/Kramer_Testimony040108.pdf (Accessed on 2 January 2011).

⁶ Ibid.

⁷ William Gibson, *Neuromancer* (New York: Ace Books, 1984), 9.

⁸ Merriam-Webster Online, <http://www.merriam-webster.com/dictionary/cyberspace> (Accessed 2 January 2011).

...all of the computer networks in the world and everything they connect and control...Cyberspace includes the Internet plus lots of other networks of computers that are not supposed to be accessible from the Internet.⁹

Another way to view or define cyberspace is by using the Open Systems Interconnection model (OSI model),¹⁰ the international standard which subdivides the digital communications into seven layers: physical (bit-level), data link (physical address), network (logical addressing), transport (connections), session (communications), presentation (capability to view), and application (data viewed by end-user).

A number of definitions for cyberspace exist across USG agencies, mostly derived from national policy documents. National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23, “*Cyber Security and Monitoring*”) defines cyberspace as “the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.”¹¹ The 2009 *Cyberspace Policy Review* expands upon its own model by noting that “common usage of the term also refers to the virtual environment of information and interactions between people,”¹² an important concept when considering the role of social media has had in the global context recently. The Department of Homeland Security (DHS) has adopted that definition for use in its 2010 *National Cyber Incident Response Plan*. The

⁹ Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins Publishers, 2010), 70.

¹⁰ This is the international standard, accepted by the International Telecommunications Union.

¹¹ *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, (Washington, DC: The White House, 2009), 1.

¹² Ibid.

2003 *National Strategy to Secure Cyberspace* defines cyberspace in the context of public and private critical infrastructures (to include government, defense industrial base, communications, transportation and energy):

Cyberspace is the nervous system of these infrastructures—the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work.¹³

Prior to 2008, the DoD (in the *National Military Strategy for Cyberspace Operations* (2006)(NMSCO)) defined cyberspace as a “domain characterized by the use of electronics and the electromagnetic spectrum (EMS) to store, modify, and exchange data via networked systems and associated physical infrastructures.”¹⁴ In May 2008, DoD adopted a definition similar to that articulated in NSPD-54:

A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.¹⁵

Daniel Kuehl, director of the Information Strategies Concentration Program at NDU, offers a more expansive definition which provides more specifics and reduces ambiguity, highlighting what distinguishes cyberspace from other environments:

A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.¹⁶

¹³ *The National Strategy to Secure Cyberspace*, (Washington, DC: The White House, February 2003), 1.

¹⁴ Daniel T. Kuehl, “From Cyberspace to Cyberpower: Defining the Problem,” in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 27.

¹⁵ DoD, JP 1-02: *DoD Dictionary of Military and Associated Terms*, (Washington: DoD, 2001, as amended through 31 January 2011), 118.

¹⁶ *Ibid.*, 28.

Kuehl argues that his definition describes cyberspace, not solely in terms of the networks and connectivity within activities, which take place within the domain, but on the “unique physical characteristics which shape it (the electromagnetic spectrum) and the actions (information being created, stored, modified, exchanged or exploited) dependent on the use of electronics and the electromagnetic spectrum which occur within it.”¹⁷ Kuehl’s definition actually ends up being a blending of the 2006 NMSCO and DoD’s revised 2008 definitions. Some have argued that the inclusion of electromagnetic spectrum in a definition on cyberspace leads to confusion with electronic warfare (defined as military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy);¹⁸ however, the emphasis on information and telecommunications networks with the cyber definitions does help distinguish between the two.

The *2011 National Military Strategy* describes cyberspace as a “globally connected domain.”¹⁹ Cyberspace is sometimes referred to as a “global common,” a shared area owned by no state, such as space or the high seas. One can draw parallels of operating in cyberspace to the open nature of the high seas, and the related need for freedom and security of operations of commercial and government activities, as well as clearly defined rules of engagement or operation.

Clarity of the definitions and reaching a common understanding associated with cyberspace pose significant challenges in the legal realm, particularly the definition over

¹⁷ Ibid., 31.

¹⁸ DoD, *Joint Publication 3-13: Electronic Warfare*, (Washington, DC: Department of Defense, January 2007), v.

¹⁹ *National Military Strategy of the United States of America 2011*, (Washington, DC: Department of Defense, 2011), 3.

what constitutes a cyber attack or use of force under international rule of law related to armed conflict. There is significant debate, nationally and internationally, as to at what point does a cyber attack reach the level of armed attack, and how do governments distinguish between attack, intrusion, exploitation or espionage activities against computer networks.²⁰ Following the 2007 cyber attacks on Estonia, a senior NATO official asked, “If a member state's communications centre is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-attack?”²¹

Given the overlap and dependencies of military/government and civilian networks, the lines between combatant and non-combatant become blurred. The law of war applies primarily to actions between states, so cyber attacks by non-state actors or individuals may not fall within the parameters of the current legal definition. The

²⁰ The United Nations defines military aggression or act of war as “the use of armed force by a State against a sovereignty, territorial integrity, or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations....” Per Article 3 of UN Resolution 3314, this includes:

- (a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;
- (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
- (c) The blockade of the ports or coasts of a State by the armed forces of another State;
- (d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
- (e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
- (f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
- (g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another.

United Nations General Assembly Resolution 3314 (XXIX), Dec. 14, 1974, <http://www1.umn.edu/humanrts/instree/GAres3314.html>, [accessed on March 6, 2011].

²¹ “Russia and Estonia: A Cyber Riot,” *The Economist*, May 10, 2007. <http://www.economist.com/node/9163598> [accessed on 25 February 2011].

international community will have to reach some consensus on cyber attacks as to when they constitute an act of war.

Key to understanding the legal implications is to understand the originator's intent and actions and the context (environment) in which the attack has occurred.²² Is the "attack" really an intrusion designed to gather information (espionage)? Espionage, or intelligence gathering, from electronic or communications sources has been going on between states for years, adapting to advances in technologies. While the intelligence collection (or the results it produces) can provide strategic, operational and economic advantages to a state during peace and war, in and of itself is not an act of war.

Or is the attack a hostile act intended to deny, degrade, destroy or disable military, government, commercial or critical infrastructures and networks? Is it part of increased tensions or hostilities between states or a random occurrence? Is it a state-sponsored effort? Activities which positively meet those criteria would likely be considered a violation under the rules of war. However, if the attack or actions are the work of individuals or criminal elements to steal or extort funds, identity or data for non-national security purposes, then those actions would likely be subject to criminal laws and prosecution.

Prior to 2001, some legal experts argued that while non-state actors could cause the same damage against a state's national security infrastructure as could state actors, hostile, transnational activity committed by a non-state actor generally remained a law

²² Franklin D. Kramer, "Cyber Security: An Integrated Governmental Strategy for Progress," Atlantic Institute Issue Brief, Washington DC, 2.

enforcement issue.²³ Since 2001, given the changing nature of armed conflict against terrorist entities (both state- and non-state supported), those non-state actors' actions can be considered under the rules of war. The same can apply to non-state actors' hostile activity in cyberspace. Similar as to how acts of terrorism are determined, the key is to understanding who the actor is and their intent. While the intent can be apparent, attributing an attack or determining the actual actor can be much more difficult (a country may be wittingly or unwittingly host to a server used to conduct an attack by a nation or actor physically located outside of that country).

Why Is the Cyberspace Domain Different?

“Cyberspace is unlike the other warfighting domains, it is a man-made technological phenomenon solely reliant upon human activity...”²⁴

There are a number of reasons as to why the cyber domain is unlike the “traditional” warfighting domains. Understanding how the domain differs from the other domains and its specific characteristics will give military and government planners a better sense of how to integrate actions across all domains to ensure freedom of action and protection of assets. Planners must also consider the unique complexities that cyberspace presents to inter-relationships and dependencies that exist between the domains.²⁵

DoD's 2010 *Quadrennial Defense Review* notes that although cyberspace is a

²³ Walter Gary Sharp, Sr., *Cyberspace and the Use of Force*, (Falls Church, VA: Aegis Research Corporation, 1999), 8.

²⁴ Keith Alexander, GEN, “Statement for the Record before the House Armed Services Committee Terrorism, Unconventional Threats, and Capabilities Subcommittee, 5 May 2009,” http://www.nsa.gov/public_info/speeches_testimonies/5may09_dir.shtml (Accessed online 31 December 2010).

²⁵ Mark E. Redden and Michael P. Hughes, *Defense Planning Paradigms and the Global Commons*, *Joint Forces Quarterly* 60 (1st quarter 2011), <http://www.ndu.edu/press/defense-planning-paradigms.html> (Accessed on 5 January 2011).

man-made domain, it is as relevant and critical a domain for military operations as the naturally-occurring domains of land, sea, air, and space.²⁶ The “traditional” domains – air, land, sea and space– exist in the natural world and their boundaries and environments are defined and for the most part, are relatively static. Technology has been developed to enable military operational capabilities and actions within each domain. Cyberspace is generally described as an artificial, man-made environment, although as noted earlier, cyberspace is bounded and defined to some extent by the physical properties of the electromagnetic spectrum in which it operates. The networks and technologies developed to operate within that environment are man-made, not unlike the ships, airplanes, vehicles or satellites developed for use in the sea, air, land, or space domains.²⁷ Rapid advances in, and convergence of, computer and information systems technology, hardware and software result in a much more dynamic and changing environment than is found in the other domains (the basic properties of the oceans or terrain features on land often remain static, absent a catastrophic event). The cyber domain, however, is constantly evolving and growing as demand and innovation drive change – new technologies such as cloud computing and small, cheaper and more capable mobile computing devices bring great opportunities and convenience, but are accompanied by increased risk, particularly from a security perspective.

Rather than existing solely as a separate environment, cyberspace (and its associated capabilities) is an integral part of the other domains, enabling capabilities and actions within those domains. Given the military’s reliance on cyber and information

²⁶ *Quadrennial Defense Review*, 37.

²⁷ Kuehl, 30.

technology, no other domain is as much a factor for successful operations as is cyberspace. It is a complex (and often insecure) network of networks with multiple national and global stakeholders across the military and government, as well as the private and public sectors. The cyber-related infrastructures and capabilities are often shared wittingly and unwittingly by those stakeholders and actions against one sector may have unintended consequences in another. Actions and rate of change in the cyber environment occur nearly instantaneously, limiting warning and decision cycles. The lag between the development of cyber attack mechanisms and the technical or security fixes creates an almost perpetual state of vulnerability, making it an imperative to get inside an actor's decision loop as early as possible.

More than any other domain, cyberspace affords actors unprecedented anonymity for actions—it can be unclear as to who is operating within the domain and their intentions—making it difficult to attribute attacks or misappropriation or manipulation of data. Cyber attacks and related actions can be asymmetric when compared to warfare or attacks within the traditional domains: the tools and capabilities necessary to undertake an attack are low-cost and can be accomplished by a single individual with appropriate, although not necessarily extensive, training and access to the Internet. A state which may be unable to counter U.S. conventional military capability could, for a relatively small investment in cyber capabilities, respond to tensions, attacks or even hold countries “hostage” by conducting cyber attacks against a critical infrastructures, such as the international financial system.²⁸

²⁸ Clarke and Knake, 259.

That disproportionate advantage of a cyber attack—for relatively low-cost investment, the results could be very expensive for the target of the attack; when coupled with the potential for anonymity of action makes cyber attack a particularly lucrative asymmetric weapon. In cyber, just as in the other domains, a situation of temporary advantage can prove decisive. Rather than a “weapon of mass destruction,” a more correct description of a cyber attack/capability may be “weapon of mass disruption,” one that is capable of precision targeting against a specific node or nodes which can result in degradation or disruption of an adversary’s capacity to operate, whether it is militarily, or in a civil capacity, such as power generation, conducting financial transactions or ensuring the security of the transportation systems. The reliance of an advanced society such as the United States on computers, the Internet and information technology in everyday life means the chaos and public fear that could result from such a well-executed cyber attack may be more effective than destruction wrought by a massive kinetic attack.

Given the dependency of U.S. military weaponry, command and control, mobility and infrastructure on cyber-enabled technology, freedom of operations in the cyberspace domain is critical to successful U.S. military operations in the other domains. General Alexander has drawn parallels between the cyber domain today and the air domain at the beginning of the 20th century:

A century ago, the world’s militaries had to learn to fight in the air...We realized that no one service can possess the entire air domain...all the services require access, all require capability, and all contribute to the joint fight. The parallels with cyberspace seem obvious: freedom of action in cyberspace, like freedom of maneuver in the air, is crucial to the efficient employment of one’s forces in all domains. Likewise, the loss of such freedom could impair the capabilities we have

built in all the other domains.²⁹

As suspected Russian operations in Estonia and Georgia and continued Chinese intrusions into U.S. military and government networks have illustrated, military planners can expect any future conflicts to include cyberspace as a theater of operations, either as part of a U.S. or an adversary's operational doctrine. There is general agreement across the USG that cyberspace is a military operational domain, although some government agencies have challenged aspects of DoD's primacy to the cyberspace domain. DHS Secretary Janet Napolitano, in remarks in mid-December 2010, stated that cybersecurity functions should be the purview of DHS and that cyberspace is "fundamentally a civilian space, and government has a role to help protect it, in partnership with the private sector and across the globe...(but) both the market and the battlefield analogies are the wrong ones to use."³⁰

The Cyber Threat: An Imperative for the United States

"...it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation."³¹

The threats posed to U.S. government and non-government networks from foreign state and non-state actors are substantial. The rapid adoption of cyber and related information technologies by U.S. military, government, financial and civil sectors worldwide have provided significant advantages in accuracy, timeliness, productivity and

²⁹ General Keith B. Alexander, Commander United States Cyber Command, speaking on the Cyber Command Posture Statement, on 23 September 2010, before the House Committee on Armed Services, 111th Cong., 2nd sess., 9.

³⁰ DHS public website, "Remarks by Secretary Napolitano at the Atlantic's Cybersecurity Forum, December 17, 2010," http://www.dhs.gov/ynews/speeches/sp_1292622750273.shtm (Accessed on 25 February 2011).

³¹ White House, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (Accessed on 9 January 2011).

connectivity. The reliance on these technologies and growing inter-connectivity makes the associated weapons, networks, infrastructures and data increasingly vulnerable to destruction or disruption from state or non-state actors, with potentially devastating consequences. Without steps to mitigate vulnerabilities and protect systems, the opportunities for attackers to disrupt telecommunications, electrical power, energy infrastructures, transportation and financial networks, and other critical infrastructures will increase exponentially.³²

Senior USG officials have increasingly highlighted the growing cyber threat to the United States from both state and non-state actors. In comments before a House Intelligence Committee in February 2011, General James Clapper, Director of National Intelligence, described the threat of cyber warfare as increasing.³³ At the same session, CIA Director Leon Panetta said cyber “represents the battleground of the future,” with the next Pearl Harbor-type event being a cyber attack that brings down the power grid, financial and government systems, effectively paralyzing the country.³⁴ To address the threat, the United States needs to develop defenses as well as put “assets in places where we can provide sufficient warning that these attacks are coming.”³⁵ As has already been seen in Georgia and Estonia, the first battleground for future conflicts will likely be in

³² ODNI, “*Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence*, 12 February 2009,” <http://intelligence.senate.gov/090212/blair.pdf> (accessed 4 January 2011).

³³ ODNI, “Statement for the Record by Director of National Intelligence James R. Clapper - Worldwide Threat Assessment of the United States Intelligence Community, 10 February 2011,” http://www.dni.gov/testimonies/20110210_testimony_hpsci_clapper.pdf (accessed 15 May 2011).

³⁴ “Cybersecurity “Battleground of the Future”, *UPI.com*, http://www.upi.com/Top_News/US/2011/02/10/Cybersecurity-battleground-of-the-future/UPI-62911297371939/#ixzz1Db8wvLWx (accessed on 10 February 2011).

³⁵ Ibid.

cyberspace.³⁶

DoD, in testimony to the House Intelligence Committee in May 2008, has claimed that U.S. military systems are scanned or attacked more than 300 million times per day.³⁷ More disturbing, cyber threats to U.S. national security extend beyond government and military networks, the systems and networks which control our civilian infrastructure upon which the government and military capabilities rely are equally, if not more so, vulnerable to disruption or attack, potentially with devastating consequences. Security experts have identified four categories of major cyber threats to national security: economic cyber espionage (one could argue that cyber espionage against military or national security systems should also be included), cyber crime (includes identity theft), cyber war, and cyber terrorism.³⁸ At present, the United States is impacted primarily by the first two categories, but over the next decade, the order may be reversed.³⁹ The 2010 *U.S. National Security Strategy* characterizes the threats to cyber as ranging from “individual criminal hackers to organized criminal groups, (and) from terrorist networks to advanced nation states.”⁴⁰

The National Intelligence Council’s most recent assessment of the future global environment, *Global Trends 2025: A Transformed World*, projects with relative certainty that the United States will see an increased use of cyber warfare attacks by state and non-

³⁶ Robert A. Miller and Daniel T. Kuehl, “Cyberspace and the “First Battle” in 21st-Century War,” *Defense Horizons* 68 (September 2009), 1.

³⁷ Eric Rosenbach, “Cyber Security and the Intelligence Community, Confrontation or Collaboration? Congress and the Intelligence Community,” http://belfercenter.ksg.harvard.edu/publication/19158/cyber_security_and_the_intelligence_community.html, (accessed on 13 January 2011).

³⁸ Joseph Nye, Jr., *Cyber Power*, (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010), 16.

³⁹ Ibid.

⁴⁰ *U.S. National Security Strategy 2010*, 27.

state actors, threatening U.S. freedom of action and expanding future conflicts beyond the traditional battlefield.⁴¹ The dependency upon, and interconnectivity of, information and cyber technologies by military communications and weapons systems and civilian critical infrastructures will dominate future warfare by the United States, our allies and adversaries. Enemy weapons systems also rely on information/cyber technology and are likewise vulnerable to attack/neutralization in a first-strike capability. Of course, the reverse is true of U.S. systems, which will require robust cyber security to maintain both defensive and offensive capability and advantage. Potential adversaries likely view cyber attacks as a means to circumvent U.S. conventional military strengths on the battlefield, choosing instead to directly attack the U.S. at home.⁴² Due to technological improvements and an increased dependence on cyberspace, the “traditional” conflict will include offensive and defensive operations in the cyberspace domain.

States pose the greatest threat to U.S. cyberspace operations. General Alexander, CDR, USCYBERCOM, indicated that foreign intelligence services pose an asymmetric threat to U.S. computer networks and China and Russia are among the “near peers” of the United States in cyber warfare capabilities.⁴³ The Intelligence Community assesses that a number of nations, including Russia and China, have the technical capacity to target and disrupt U.S. information technology infrastructure and exploit that infrastructure for intelligence collection.⁴⁴ Russia and China are suspected of conducting cyber attacks

⁴¹ National Intelligence Council, *Global Trends 2025: A Transformed World* (Washington, DC: Office of the Director of National Intelligence, 2008), 71.

⁴² *Ibid.*, 97.

⁴³ “Cyber Threat to Pentagon is Global: China, Russia Near Peers of US,” *Grendel Report Online*, 1 October 2010, <http://grendelreport.posterous.com/cyber-threat-to-pentagon-is-global-china-russ> (accessed on 5 January 2011).

⁴⁴ ODNI, “Annual Threat Assessment.”

penetrating DoD computer networks, to include non-networked and defense industrial base (DIB) systems. Pentagon officials suspect that computer hackers working from Russia struck U.S. Central Command computers in 2008 and involved malicious software, known as "malware," that permeates a network.⁴⁵ The malware was reportedly introduced by peripherals, namely USB or "flash" drives, which then spread undetected on classified and unclassified systems, allowing attackers to transfer data out of the network to servers under foreign control, breaching the secure and non-secure systems.⁴⁶

Russia is suspected of using cyber attacks to achieve political and military objectives in several recent events. Russian government sources are believed to be behind a series of distributed denial-of-service attacks which targeted Estonian web servers in 2007, following a dispute over Estonia's removal of a Soviet World War II war memorial. The attacks, which lasted for several weeks, effectively paralyzed the country's government, disabling the websites of Estonian government ministries, political parties, newspapers, banks, and companies.⁴⁷

In August 2008, in support of its military invasion of Georgia, Russia is suspected of conducting coordinated cyber attacks on Georgian government, media and public websites. The attacks, while not directly attributed to Russian government sources, severely inhibited the Georgian government's ability not only to conduct effective

⁴⁵ Alex Spillius, "Russian Hackers Penetrate Pentagon Computer System in Cyber Attack," *The Telegraph*, 30 November 2008, <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/3535165/Russian-hackers-penetrate-Pentagon-computer-system-in-cyber-attack.html> (accessed 4 January 2011).

⁴⁶ Angela Moscaritolo, "Pentagon Official Reveals "Most Significant" Military Breach," *SCMagazine*, <http://www.scmagazineus.com/pentagon-official-reveals-most-significant-military-breach/article/177586/> (accessed on 8 January 2011).

⁴⁷ Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, 17 May 2007, <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia> (accessed on 4 January 2011).

command and control of its government and military forces, but also limiting its ability to disseminate information to the rest of the world. The cyber attack began with denial-of-service attacks which crippled Georgia's infrastructure, to include its entire governmental decision-making apparatus. The cyber attacks were a precursor to actual ground operations and continued throughout the two-week conflict.

China perhaps represents the most significant state threat currently to U.S. cyberspace activities. In recent statements, Chairman of the Joint Chiefs of Staff, ADM Mike Mullen, has asserted that China poses a significant threat to cyber security.⁴⁸ China has incorporated information dominance into its current and future defense strategies and recognizes the importance of cyberspace operations to understanding the current strategic "battlefield" as well as in shaping future conflicts. China is investing significant capital, particularly military resources, into its computer network exploitation capabilities to support strategic intelligence collection objectives and lay the foundation for success in potential future conflicts.⁴⁹ Chinese defense theorists have opined that China's military future is not in competing to build aircraft carriers, but in advanced weapons, to include cyberspace operations, to "make other command systems fail to work."⁵⁰ In 1999, two senior Chinese military officers published a book, *Unrestricted Warfare*, outlining the use of asymmetric warfare capabilities, to include network or cyber attack capabilities, to defeat a militarily superior adversary. They describe how the advantage can be obtained,

⁴⁸ Charley Keyes, "Mullen: Cyber attack potential impact 'substantial'," *CNN Tech*, January 12, 2011, http://articles.cnn.com/2011-01-12/tech/cyber.threat_1_cyber-attack-cyber-command-threats?s=PM:TECH (accessed on 15 January 2011).

⁴⁹ Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, prepared for the US-China Economic and Security Review Commission*, (McClean, VA: Northrup-Grumman, 2009), 6.

⁵⁰ David Ignatius, "The Future of Warfare," *Washington Post*, January 2, 2011.

not by direct force-on-force attacks, but by attacking “softer” centers of gravity, using such methods as activating a previously buried computer virus to disable and paralyze the country’s financial or transportation sectors.⁵¹

U.S. government officials and media have cited repeated Chinese attacks on U.S. government, public and private networks since at least early 2000. China has already conducted a number of “attacks” against or, perhaps, more correctly, “intrusions” or “espionage,” primarily designed to gain information about or data from U.S. government, military and defense industry websites. China’s manipulation (to include blocking and redirection) of U.S. non-government servers and websites, to include the mega networking site Google, enables its control and targeting of corporate and intellectual property and knowledge, further raising concerns over its intentions and capabilities.⁵² In April 2010, China’s state-controlled telecommunications company hijacked reportedly 15 percent of the world’s Internet traffic, including data from U.S. military, civilian organizations and those of other U.S. allies.⁵³

Other aspects of Chinese activity related to the cyber domain also raise concern. Potential Chinese agents’ infiltration of critical USG agencies, such as the Department of Energy (DOE), poses a significant risk to open and restricted computer systems and information, according to DOE officials. China has a supercomputing and component manufacturing capability, which rivals if not exceed, that of the United States. Chinese

⁵¹ Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China’s Master Plan to Destroy America*, (Panama City, Panama, Pan American Publishing Company, 2002 (translated version)), 123.

⁵² In early 2011, China used its cyber capabilities and controls to censure the ability of pro-democracy activists to use the Internet and other media to organize protests (called the “Jasmine Revolution”) in the wake of the successful use of social media in the Middle East uprisings.

⁵³ Joshua Miller, “Internet Traffic from U.S. Government Websites Was Redirected Via Chinese Networks, 16 November 2010,” *FoxNews Online*, <http://www.foxnews.com/politics/2010/11/16/internet-traffic-reportedly-routed-chinese-servers> (accessed 5 January 2011).

influence over, and the latent threat potentially residing in, the computer technology, hardware and software supplied by the Chinese-dominated computer technology industry have yet to be fully understood by U.S. analysts. Exploitation and attack tools/capabilities can be implanted undetected during the manufacturing process, to be activated at a time and place of the actor's choosing. Cybersecurity policies and practices will also need to address supply-side security, if technology, particularly that adopted by military and government end-users, is acquired from overseas manufacturers.

In addition to the threats that state actors pose, U.S. officials remain equally concerned over the threats posed by non-state entities, to include terrorist organizations, organized criminal groups, or individual actors. Criminal elements are becoming increasingly technically competent and continue to target government and private sector information and financial networks to gain competitive advantage or steal financial data or funds.⁵⁴ Terrorist groups, including al-Qa'ida, HAMAS, and Hizballah, have expressed the desire to use cyber means to target the United States.⁵⁵ The Central Intelligence Agency believes terrorists will continue to pursue traditional attack methods, but anticipates the risk of cyber threats will increase as a more technically competent generation joins those groups.⁵⁶ Currently, terrorist entities are taking advantage of cyberspace to maintain connectivity beyond safehavens, coordinate activities, conduct information campaigns, and radicalize and recruit new members.

⁵⁴ ODNI, "Annual Threat Assessment."

⁵⁵ Ibid.

⁵⁶ Government Accountability Office, *Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk*, (Washington, D.C.: Government Accountability Office, 2009), 4.

Individuals typically characterized as hackers or hacktivists,⁵⁷ with malicious intent, whether driven by political or ideological reasons or for personal gain or satisfaction, can also pose a significant threat to U.S. government, military and commercial networks. Insiders, either foreign intelligence agents or employees motivated for various reasons (disgruntled, political, ideological) represent serious threats to cyber networks and infrastructure. These individuals may have trusted access to intranet, closed or secure networks, and the disruption or misappropriation of information from these sources can have significant national security consequences (for example, the 23-year old Army specialist accused of providing volumes of classified State Department cables to Wikileaks).

Social media networks provide an effective mechanism to unify and organize civil populace actions and uprisings against a standing government, as has played out during the 2009 Iranian elections and most recently in Tunisia, Egypt and Libya in early 2011. While this is not a cyber “threat” per se, the ability to manipulate and use cyber-related capabilities, such as the Internet or associated social media applications (i.e., Facebook, Twitter, YouTube), to effect civil disobedience or regime change, or correspondingly, the restrictions and censorship a threatened government may place on a population to access and use the Internet or other cyber-assisted technology, have significant ramifications to U.S. national security interests. There is a perception among some non-Western governments that social media is being manipulated by the U.S. in particular to achieve

⁵⁷ These terms are sometimes used interchangeably, however hackers often are individuals who crack into networks for the thrill of the challenge or for bragging rights in the hacker community, while hacktivists, either individually or as part of a group, conduct politically motivated attacks on publicly accessible Web pages or email servers. GAO, *Cyber Threats and Vulnerabilities Place Federal Systems at Risk*, 4.

its goals. The rapid and viral nature of the spread of unrest will present challenges for U.S. diplomatic and policy efforts. It requires intelligence capabilities, well-postured to detect and monitor signs of unrest and manipulation within those venues, to provide timely situational awareness and information to U.S. decision-makers, as well as policies designed to clarify the human rights nature of Internet access and censorship.

CHAPTER 2: STRATEGIC DIRECTION AND KEY PLAYERS

“The cyber domain is new, and policy has not caught up to reality. Government and private officials are grappling with basics such as what constitutes a cyber attack and who has responsibility to defend against threats...who does what and when they do it is under discussion with other government agencies.” DASD Cybre Policy, Robert Butler ¹

The USG’s response to the cyber threat and efforts to ensure that the U.S. maintains uninterrupted access to the cyber/digital environment for government and private services spans across all elements of the government and commercial sectors. The strategic direction for the USG response to cyber threats is derived from national-level strategies and is reflected in our defense, diplomatic, homeland security, and law enforcement strategies, organizations and actions. The degree to which each department/agency has implemented a cyber strategy and its respective roles and responsibilities varies significantly; some, such as the DoD and Department of Homeland Security (DHS), are fairly mature in their development, others, like the Department of State, are just beginning to define their strategies and organizational structures. The ability for all of the departments and agencies to organize, develop and synchronize their efforts is critical to the overall USG effort to ensure freedom of operations in the cyber environment.

Traditional roles and responsibilities for the defense of national assets and the U.S. population from foreign attacks are being revised for cyber. The military is responsible for the defense of all U.S. interests and the homeland from enemy (state-sponsored) attacks with conventional weapons. In the cyber realm, however, DoD is

¹ Jim Garamone, “Official Details DOD Cybersecurity Environment,” *American Forces Press Service*, <http://www.defense.gov/News/NewsArticle.aspx?ID=61356> (accessed on 13 January 2011).

responsible only for the defense of those networks associated with the military or defense industrial base, while DHS is responsible for federal networks and U.S. critical infrastructure, and theoretically, industry for the private sector networks. While those efforts should provide effective deterrence against foreign attacks, the currently nascent, and often fragmentary, nature of the approach limits the effectiveness of the USG cybersecurity efforts. Reaching consensus in determining the roles, responsibilities, authorities and accountability of each organization is crucial to establishing unity of effort and presenting a strong national deterrent capability.

National-level Direction and Engagement

At the national-level, direction related to addressing the cyber threat and maintaining U.S. capabilities to operate freely in cyberspace has been an underlying theme in policy statements and guidance over the past two Administrations. The Comprehensive National Cybersecurity Initiative (CNCI) was adopted as policy under the 2008 National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23, *Cyber Security and Monitoring*) and outlines how the USG plans to protect cyber and its associated infrastructure as a national strategic asset. The CNCI addresses current and future cybersecurity threats, while seeking to mitigate vulnerabilities and provide long-term strategic operational and analytic capabilities, through investment in USG capabilities as well as through emphasizing public-private partnerships.² The 2010 *National Security Strategy (NSS)* highlights U.S. national security, economic and critical infrastructures' capabilities and reliance afforded by cyber

² 2010 *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence*, (Washington, D.C.: Office of the Director of National Intelligence, 2010), 4.

technologies and the potential vulnerabilities to state and non-state threats we face as a result of that reliance. The President has made the nation’s cyber/digital infrastructure a “strategic national asset, and protecting it—while safeguarding privacy and civil liberties—is a national security priority.”³ The NSS outlines two primary areas of emphasis to deter, prevent, detect, defend and recover from cyber intrusions and attacks: 1) investment in people and technology, working across the government and private sector to design more secure technology; and 2) strengthening partnerships, both nationally and internationally.⁴

Early in his first year in office, President Obama directed a 60-day Cyber Policy Review to assess U.S. policies and infrastructures to address and respond to cyber threats. That review resulted in 24 recommendations (see Appendix 1 for a listing of the 24 recommendations); however, in October 2010, a Government Accounting Office (GAO) review noted that the U.S. Government was making slow progress in all but two of the 24 specific goals highlighted in the report.⁵ One of the policy review recommendations was to appoint a cybersecurity policy official within the National Security Council (NSC)(Special Assistant to the President and Cybersecurity Coordinator) who would be responsible for coordinating the nation’s cybersecurity policies and activities.

President Obama appointed the first U.S. cybersecurity coordinator, Howard Schmidt, in December 2009, as an affirmation of the Administration’s commitment to

³ *The National Security Strategy of the United States*, (Washington, DC: White House, 2010), 27.

⁴ *Ibid.*, 28.

⁵ A detailed status of the recommendations can be found in GAO-11-24, *Executive Branch is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership is Needed*, (Washington, D.C.: GAO, October 6, 2010), <http://www.gao.gov/products/GAO-11-24> (accessed on 28 November 2010).

provide cybersecurity the "high-level focus and attention" necessary to counter threats and protect the government, military and private sectors from growing cyber attacks by adversaries.⁶ The previous administration had several "senior directors" for cyberspace at the NSC-level, but this new position portrays more proactive administration involvement on cyber issues. The cybersecurity coordinator leads a new Cybersecurity Directorate within the NSC and works with federal agencies, as well as state, local and private organizations. Schmidt, in initial remarks, identified his priorities as articulated by the President:

- Developing a new comprehensive strategy to secure American networks
- Ensuring a organized unified response to future cyber incidents
- Strengthening public, private and international partnerships
- Promoting research and development of the next generation of technologies
- Leading a national campaign to promote cybersecurity awareness and education⁷

According to the White House website, as of July 2010, the NSC's Cybersecurity Directorate was in the process of updating NSPD-54/HSPD-23, a classified directive released in January 2008 by the Bush Administration. The revised Presidential Directive reportedly will further incorporate the recommendations outlined in the Cyber Policy Review and evolve the CNCI activities into a broader U.S. cybersecurity strategy.⁸ As part of the revisions, the Administration will seek to define clearly the roles and

⁶ Jaikumar Vijayan, "Obama Outlines Cybersecurity Plans, Cites Grave Threat to Cyberspace," *ComputerWorld Online*, http://www.computerworld.com/s/article/9133653/Obama_outlines_cybersecurity_plans_cites_grave_threat_to_cyberspace (accessed on 9 January 2011).

⁷ Dan Raywood, "Obama Identifies Five Priority Areas for the New Cybersecurity Coordinator," *SC Magazine Online*, <http://www.scmagazineuk.com/president-barack-obama-identifies-five-priority-areas-for-the-new-cybersecurity-coordinator-howard-schmidt-as-he-is-greeted-with-a-positive-response/article/160219/> (accessed on 8 January 2011).

⁸ White House, "Cybersecurity Progress after President Obama's Address, 14 July 2010," <http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010> (accessed on 13 January 2010).

responsibilities across USG entities for cyberspace actions and to ensure policies, laws and authorities allow those entities to carry out the responsibilities allocated to them. The Cybersecurity Directorate is to identify a mitigation strategy to overcome the challenges and shortcomings facing progress on CNCI initiatives identified by a March 2010 GAO study, to include: defining roles and responsibilities; establishing measures of effectiveness and an appropriate level of transparency; reaching agreement on the scope of educational efforts; coordinating actions with international entities and coalitions; and strategically addressing identity management and authentication.⁹ Activities to mitigate these shortcomings will play into an overall USG strategy to effectively integrate the USG efforts to defend and operate securely in cyberspace.

Congress

Congress is not remaining a sideline player on cyber issues. Much of the oversight for cyber issues being conducted by Defense and other USG departments is provided through the respective standing House and Senate Intelligence, Armed Services, and Homeland Security committees, although there is not a single committee with primary jurisdiction. A 2009 Congressional Research Service report asserted that while “many different initiatives exist, the fragmentation of missions and responsibilities, “stove-piping,” and lack of mutual awareness between stakeholders, makes it difficult to ascertain where there may be programmatic overlap or gaps in cybersecurity policy.”¹⁰ A

⁹ *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338, (Washington, D.C.: Government Accounting Office, March 2010), ii.

¹⁰ Catherine A. Theohary, “Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress,” *Congressional Research Service*, September 30, 2009, <http://www.fas.org/sgp/crs/natsec/R40836.pdf>. (accessed on 13 January 2011).

House Cybersecurity Caucus was established in September 2008 with a goal to “raise awareness and provide a forum for members representing different committees of jurisdiction to discuss the challenges in securing cyberspace,”¹¹ although it does not appear to carry much legislative authority.

Recent Congressional legislation, while forward-leaning, has run into roadblocks related to privacy and civil liberties concerns. Numerous legislative initiatives related to the security of USG systems, critical information infrastructure and other non-federal systems, have attempted to fix flaws in the cyber infrastructure and processes. Much of the legislation is reactive, such as to allegations that USG and military sites were “erroneously hijacked,” or all traffic was re-routed through, Chinese servers in April 2010. However, only limited legislation has been enacted to date, mostly in provisions under the National Defense Authorization and Intelligence Authorization Acts, although newly proposed legislation in April 2011 will provide broader authorities to some agencies and strengthen U.S. cybersecurity.

Key Players:

DoD (and by extension, USCYBERCOM); DHS and the National Security Agency are really the linchpins in the USG’s cyberspace efforts. While other USG organizations have key roles to play in the cyberspace, particularly in the defensive arena, leadership and synchronizing capabilities will be driven by the DoD and DHS.

DoD

“DoD has a large [information technology] IT footprint. We operate more than 15,000 networks within the .mil domain. We have seven million computing

¹¹ Congressional Cybersecurity Caucus Website, <http://cybercaucus.langevin.house.gov/> (accessed on 14 January 2011).

devices. We rely not only on our own networks, but also on many commercial and government networks outside the .mil domain. The fact is that our Department depends on the overall IT infrastructure of our nation.”¹²

Secretary Lynn’s remarks above, while highlighting the reliance of DoD on IT, barely conveys the extent to which the military’s weapons, command and control, and logistics systems rely on military, government or commercial information technology or cyber infrastructure. Virtually every aspect of daily, tactical or strategic military operations and activities access or rely on IT/cyber infrastructure, whether on open or closed networks. Nearly 90 percent of DoD communications use the commercial internet backbone. That reliance, with implications across the operating capacity of all domains, highlights vulnerabilities to exploitation, manipulation or degradation by an adversary. Given the global nature of cyber, however, our key adversaries have similar vulnerabilities, opening up opportunities for the military and USG.

The most recent *National Defense Strategy*, published in 2008, acknowledges the threats and risks posed by cyber, but provides little specifics as to how to defend against the threats or mitigate risks. The *2010 Quadrennial Defense Review* (QDR) identifies operating effectively in cyberspace as a key mission for the military. In order to achieve that ability to operate freely in cyberspace, the QDR highlighted four areas for investment and emphasis: developing a comprehensive approach to DoD operations in cyberspace; developing greater cyberspace expertise and awareness; centralizing command of

¹² William J. Lynn III, “2010 Cyberspace Symposium: Keynote – DoD Perspective, 26 May 2010.” http://wstiac.alionscience.com/pdf/eNews_CW_052610.pdf (accessed on 8 January 2011).

cyberspace operations; and enhancing partnerships with other agencies and governments.¹³

The recently released 2011 *National Military Strategy* calls for a cyberspace capacity which enables the military to “operate effectively across all domains.”¹⁴ To achieve this, the strategy calls for military commands to collaborate across a spectrum of government and non-government, industry and foreign entities; provide support in response to a large cyber attack; and seek new authorities to enable effective cyberspace operations.¹⁵

Building and enhancing relationships with interagency, industry and international partners are central themes across all DoD cyber efforts, recognition that collaboration with other organizations is mutually beneficial to the military and supporting partners, ensuring that both retain the ability to operate in cyberspace. The QDR identifies information sharing, support for law enforcement, defense support to civil authorities and specifically calls out cooperation with DHS, as critical areas for partnership development.¹⁶

At the DoD-level, the Office of the Deputy Assistant Secretary of Defense (DASD) for Cyber Policy is the primary office responsible for developing and overseeing the implementation cyber-related policies, strategies, and plans related to cyber action in support of US national security objectives.¹⁷ The current DASD for Cyber Policy, Robert

¹³ *Quadrennial Defense Review*, 38.

¹⁴ *National Military Strategy*, 10.

¹⁵ *Ibid.*, 10.

¹⁶ *Quadrennial Defense Review*, 38-39.

¹⁷ DOD website, “Office of the Deputy Assistant Secretary of Defense for Cyber Policy,” <http://policy.defense.gov/gsa/cp/index.aspx> (accessed on 5 January 2011).

Butler, has emphasized that partnerships among the interagency community, international partners and across industry are critical to the successful execution of a military strategy on cyber.

United States Cyber Command

Key to the DoD's strategy to centralize command of cyberspace operations has been the creation of a new command, U.S. Cyber Command (USCYBERCOM). The White House hailed the establishment of USCYBERCOM as a unifying and strengthening effort of DoD efforts,¹⁸ as well as a forcing function to integrate cyberspace operations across the USG. The creation of a military organization specifically responsible for cyber defense and operations is a key component of a credible deterrent strategy to protect against cyber attacks.

Prior to 2010, the military's operational cyber activities were led by several joint activities, primarily the Joint Task Force-Global Network Operations (JTF-GNO), under the Defense Information Systems Agency (DISA), and Joint Functional Component Command-Net Warfare (JFCC-NW), under U.S. Strategic Command (USSTRATCOM) (led by the Director, NSA). In 2009, to improve unity of effort and optimize scarce resources, Secretary of Defense Robert Gates ordered the creation of a new military command to coordinate the military's cyberspace efforts. In his memo directing the creation of the command, Gates noted that the command needed to be "capable of

¹⁸ National Security Council, "Cybersecurity Progress after President Obama's Address, 14 July 2010," <http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010> (accessed on 13 January 2010).

synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners.”¹⁹

USCYBERCOM, which achieved initial operating capability in May 2010 and declared full operational capability in November 2010,²⁰ is the centerpiece of DoD’s effort to ensure freedom of action in, and security of, the cyberspace domain. The command has responsibility to protect and defend all networks characterized as part of the “.mil” domain as well as other networks, such as those associated with military educational institutes or the defense industrial base which may not use the .mil domain, but are affiliated with U.S. DoD or military activities. It can also conduct offensive operations in cyberspace upon order. Deputy Secretary of Defense William Lynn described the mission of USCYBERCOM as “leading the day-to-day defense of all military networks, support military and counterterrorism missions, and under the leadership of the Department of Homeland Security, assist other government, civil authority and industry partners.”²¹

As recommended by Secretary Gates, the commander of USCYBERCOM is “dual-hatted” as the Director of the NSA. While it is not unusual for a commander to be “dual-hatted,” his assignment has caused consternation in some circles because of the cross-over this represents between authorities (military under USC Title 10 and foreign intelligence under USC Title 50) and the potential conflict of interest the two represent.

¹⁹ DoD Memorandum, “Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Forces Command for Military Cyberspace Operations,” (Washington, D.C.: DoD, 23 June 2009). <http://online.wsj.com/public/resources/documents/OSD05914.pdf> (accessed on 8 January 2011).

²⁰ DoD Website, “Cyber Command Achieves Full Operational Capability, 3 November 2010,” <http://www.defense.gov/releases/release.aspx?releaseid=14030> (accessed 5 January 2011).

²¹ Keith Alexander, GEN, “Mission Success in Cyberspace,” *MIT* Volume 14, issue 6 (July 2010). <http://www.military-information-technology.com/mit-home/261-mit-2010-volume-14> (accessed 12 September 2010).

General Alexander has described the relationship between NSA and USCYBERCOM as the “intersection of military, intelligence and information assurance capabilities.”²²

USCYBERCOM’s mission is to “plan, coordinate, integrate, synchronize and conduct activities to direct the operations and defense of specified DoD information networks and; prepare to, when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./allied freedom of action in cyberspace and deny the same to our adversaries.”²³ USCYBERCOM provides centralized command of all DoD cyberspace operations, strengthens DoD cyberspace capabilities and integrates DoD’s cyber expertise across the Services.²⁴

Upon request, USCYBERCOM can assist other USG elements, although under DHS leadership. General Alexander acknowledged in September 2010 that the issues of defining roles and responsibilities between USCYBERCOM, the rest of DoD, the Intelligence Community and DHS have to be clarified and delineated.²⁵ That delineation would better enable the USG to work as a team on cyber issues. General Alexander has also put forward the concept of a “dot secure” network, a separate secure network or zone that would encompass not only military and government networks, but also private ones critical to the nation’s well-being, such as banks, power grids and defense companies working on vital technologies.²⁶ The reality of the interdependencies of DoD and USG networks on each other and commercial networks make such a network unlikely,

²² Alexander, “Mission Success in Cyberspace.”

²³ US CYBERCOM Fact Sheet, as posted on the US STRATCOM website, <http://www.stratcom.mil/factsheets/cc/> (accessed on 5 January 2011).

²⁴ Ibid.

²⁵ Jack Moore, “Cyber Hearings Wrap-Up: Uncertain Road toward Secure Zone,” *ExecutiveGov*, September 24, 2010, <http://www.executivegov.com/2010/09/cyber-hearings-wrap-up-uncertain-road-toward-secure-zone/> (accessed on January 16, 2011).

²⁶ Ibid.

logically, physically and most importantly, fiscally.

Department of Homeland Security

While DoD is responsible for the security of the “.mil” domain and related defense industrial base networks, the Department of Homeland Security (DHS) is responsible for the protection of the other federal government networks and U.S. critical infrastructure as directed. DHS also is the lead agency for domestic cyber incident response, operates the United States Computer Emergency Readiness Team (US-CERT), and oversees implementation of the Trusted Internet Connection initiative.

The 2008 Comprehensive National Cybersecurity Initiative (CNCI) identifies DHS as the lead agency for securing the civilian federal government networks (.gov) outside of those under DoD purview. In July 2010, OMB clarified DHS’s role related to security of Federal information systems, directing that DHS will exercise primary responsibility within the executive branch for the operational aspects of federal agency cybersecurity with respect to the federal information systems that fall under the *Federal Information Security Management Act of 2002 (FISMA)*.²⁷

Additionally, DHS works closely with state and local authorities, public utilities and vulnerable industries, such as the chemical sector, to raise awareness and institute safeguards, especially to protect the Supervisory Control and Data Acquisition (SCADA) systems which control the operations of the utilities and plants which provide basic services to the U.S. public. DHS officials acknowledge that the cyber problem is extensive and difficult, and a lot of work still needs to be done to clarify the roles and

²⁷ Office of Management and Budget Memorandum, “Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),” (Washington, D.C.: Office of Management and Budget, 6 July 2010).

responsibilities and identify the capabilities necessary for USG agencies to successfully address the problem.

Although she has claimed that cybersecurity functions for the USG should fall primarily under the purview of DHS, Secretary Napolitano has acknowledged that DHS must coordinate with DoD and industry in order to protect cyberspace. Further, DHS recognizes that it does not have the resources necessary to assume full responsibility for cybersecurity across the USG and U.S. critical infrastructure. In October 2010, Secretary Napolitano and Defense Secretary Robert Gates signed a memorandum of agreement (MOA) which improves the coordination between the two organizations and enables sharing of personnel and tools which will enhance the security of U.S. cyber and critical infrastructures.²⁸ In particular, it enables DHS to take advantage of DoD's cyber expertise and brings the strength of NSA's cryptologic and technical capacity to defend USG and critical national systems.²⁹ Under terms of the agreement, DHS Deputy Assistant Secretary for Cybersecurity and Communications, RADM Michael Brown, will work at NSA along with other DHS personnel, including officers specializing in legal and privacy issues.³⁰ The two organizations will create a "Joint Coordination Element" under

²⁸ This MOA is unique and represents a significant policy change. Under the *Posse Comitatus* Act, U.S. forces are prohibited from acting in a law enforcement capacity within the United States, except when expressly authorized by the Constitution or Congress, unless in response to a natural disaster as declared by the President of the United States. Proponents of the policy shift argue that the majority of the USG's computer network defense capabilities reside in the DoD, while many key targets of an adversary likely would be on domestic soil.

²⁹ "DHS, DoD to Tackle Jointly Cyber Defense," *GovInfo Security*, October 14, 2010. http://www.govinfosecurity.com/articles.php?art_id=3010 (accessed 13 January 2011).

³⁰ J. Nicholas Hoover, "Homeland Security, Defense Sign Cybersecurity Pact," *Information Week Government*, October 14, 2010. <http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=227800034> (accessed on 25 February 2011).

Brown to facilitate joint operational planning.³¹

To address the expanse of systems currently under its purview, DHS has established the office for Cybersecurity and Communications (CS&C), which is responsible for enhancing the security, resiliency and reliability of the nation's cyber and communications sectors. The CS&C carries out its mission through its three divisions, the most relevant to the cyber issue being the National Cyber Security Division (NCSD). The NCSD, responsible for protecting the nation's cyber infrastructure has two strategic objectives: build and maintain an effective national cyberspace response system, and implement a cyber-risk management program for protection of critical infrastructure.³² NCSD works to achieve its strategic objectives through a number of programs, to include National Cyberspace Response System, which includes the National Cyber Alert System; the US-Computer Emergency Readiness Team (US-CERT); the National Cyber Response Coordination Group (NCRCG), which is the principal federal agency mechanism for cyber incident response; and the Cyber Cop Portal, an information sharing and collaboration tool used for coordination with law enforcement.³³

US-CERT is the operational arm of the NCSD, responsible for providing incident response and defense against cyber attacks on the .gov networks. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public.³⁴

³¹ Ibid.

³² National Cyber Security Division Website, "National Cyber Security Division," http://www.dhs.gov/xabout/structure/editorial_0839.shtm (accessed on 14 January 2011).

³³ Ibid.

³⁴ U.S. CERT Website, "About Us," <http://www.us-cert.gov/aboutus.html> (accessed on 14 January 2011).

US-CERT facilitates information sharing and collaboration through working groups which include federal, state and local government, industry and international participation.³⁵

DHS also runs the National Cybersecurity and Communications Integration Center (NCCIC), a 24-hour operations center run which provides threat warning and analysis to protect the nation's critical information technology infrastructure. The NCCIC combines the efforts of U.S.-CERT and the National Coordinating Center for Telecommunications. Under the terms of the recent DoD-DHS Memorandum of Agreement, DoD will provide cyber analysts to help run the NCCIC.

In July 2010, OMB and the White House assigned DHS the responsibility for overseeing USG departments and agencies' compliance with information assurance (to include cybersecurity) under FISMA.³⁶ Additionally, DHS is also charged with the oversight of the government-wide implementation of cybersecurity policies. It is not clear to what extent DHS will have oversight over DoD systems, although national security of classified and Intelligence Community systems fall under the oversight of NSA rather than FISMA. As of early April 2011, there is draft legislation to give DHS broader oversight over civilian agency networks, with the same authorities for the .gov networks that DoD has for the .mil networks.³⁷ The bill would also give DHS the FISMA

³⁵ U.S. CERT Website, "Government Users," <http://www.us-cert.gov/federal> (accessed on 14 January 2011).

³⁶ Angela Moscaritolo, "White House Office Grants DHS Cybersecurity Oversight," *SC Magazine*, <http://www.scmagazineus.com/white-house-office-grants-dhs-cybersecurity-oversight/article/174442/> (accessed on 13 January 2011).

³⁷ Jason Miller, "White House Draft Bill Expands DHS Cyber Responsibilities," *Federal News Radio*, 14 April 2011, <http://www.federalnewsradio.com/?nid=35&sid=2345684> (accessed on 15 April 2011).

authorities currently under OMB and establish a National Center for Cybersecurity and Communications at DHS (probably with a broader mandate than the current NCCIC).

National Security Agency (NSA)

The NSA, a DoD Combat Support Agency and a member of the Intelligence Community, has two primary missions: Signals Intelligence (SIGINT) and Information Assurance (IA). Both mission areas are critical components to the USG's cyber efforts. The SIGINT mission collects, processes, and produces intelligence from foreign signals in support of policy-maker requirements and military operations. The IA mission develops products and capabilities to protect and prevent unauthorized access to U.S. national security information systems. As part of the IA mission, the Director NSA is the designated National Manager for the security of National Security Systems in accordance with National Security Directive 42.³⁸ NSA's National Threat Operations Center (NTOC) is responsible for monitoring global networks to identify network-based threats and protect U.S. and allied networks. The NTOC establishes real-time network awareness and threat characterization capabilities to forecast, alert, and attribute malicious activity and enable coordination of computer network operations by NSA, DoD and other mission partners.³⁹ To support the SIGINT and IA missions, NSA maintains a vast technical, collection and analytic architecture which is optimized to enable the breadth of computer network operations.

General Alexander has described the relationship between NSA and USCYBERCOM as the "intersection of military, intelligence and information-assurance

³⁸*National Cyber Incident Response Plan*, (Washington, D.C.: Department of Homeland Security, 2010), 6.

³⁹ *Ibid.*

capabilities,”⁴⁰ a critical component of the nation’s cybersecurity strategy. Part of the rationale for the close relationship (to include co-location and the shared leadership) between NSA and USCYBERCOM is the ability for USCYBERCOM to leverage NSA’s resident and extensive technical collection and analytic infrastructure to support its offensive and defensive cyberspace operations within the parameters of authorities and legal rights. NSA also has developed a close relationship with other agencies, such as DHS, to provide cybersecurity support. By not replicating the capabilities and infrastructure, it enhances unity and coordination of efforts, improves timely sharing of information, and is a more efficient stewardship of limited government resources.

Other Organizations and Efforts

Beyond the organizations identified above, there are a number of departments and agencies across the USG, to include the Departments of State, Justice, and the Intelligence Community, as well as at the state, local, and commercial/industry sectors, which have significant responsibilities related to the operations and security of the nation’s cyber/digital infrastructure and capabilities. Foreign partners also play a key role in supporting the U.S.’s ability to operate in and secure cyberspace. Appendix 2 includes a table summarizing key organizations and foreign partners engaged in cyberspace operations and provides more details on various USG organizations structure and activities related to cyber.⁴¹

⁴⁰ GEN Alexander Speech, 3 June 2010, as posted on the NSA website, http://www.nsa.gov/public_info/files/speeches_testimonies/100603_alexander_transcript.pdf (accessed on 30 January 2011).

⁴¹ See Appendix 2, which begins on page 80.

Despite the breadth of organizations and partners efforts related to cyberspace operations, their efforts are generally uncoordinated and complex, and at best, loosely federated. Each agency has different strategic objectives in conducting its cyberspace operations and operates under different authorities, which creates gaps and seams in the overall USG cyber posture. Sharing of critical information is often inhibited by classification or other restrictions, there is duplication of effort, and a consolidated and coherent cyberspace situational awareness is not consistent or mature across all agencies. It would be advisable to create a separate department, activity or organization to take the lead in managing and directing the USG efforts related to cyber. There are efficiencies and operational advantages to having an agency or organization whose sole focus is cyber and which can coordinate, synchronize and integrate all USG efforts and the relations with foreign and industry partners. The danger comes if that agency or organization is created with no clear authorities, responsibility, accountability or resources (including budgetary), making it a “hollow” infrastructure. An alternative would be to create a strong interagency task force, under the direction and leadership of the NSC/Cybersecurity Coordinator.

CHAPTER 3: ISSUES AND CHALLENGES

“Unlike the sea, air, land and space domains, cyber is not an area where military power alone can dominate...Working together is not only a national imperative...it is also one of the great technical challenges of our time.” D/Sec Def William Lynn¹

There are a number of challenges which the DoD faces in being able to ensure its ability to operate in a position of superiority and securely in the cyberspace domain, whether singularly or as part of a whole-of-government effort. To ensure freedom of operations in the cyber domain, military planners will need to develop plans which address the military aspects of cyberspace operations, as well as consider and incorporate the impacts cyber actions or war will have on national, economic, critical infrastructure and society. As the previous chapter outlined, there are a number of stakeholders who have responsibilities and authorities to defend or conduct operations within cyberspace.

Some of the challenges facing an effective whole-of-government approach include establishing national policy and leadership to unify and synchronize USG efforts, delineating roles and responsibilities, instituting standard definitions and rules of engagement, establishing appropriate authorities and laws which enable action while protecting privacy and civil liberties, and enhancing information sharing and partnerships. As the USG looks beyond just a USG-centric approach, incorporating industry, the private sector and international partners, additional issues arise. The relative “newness” of cyber as a national security issue, the immaturity of USG policies and

¹ Karen Parrish, “Lynn Urges Partnership Against Cyber Threat,” *Armed Forces Press Service*, February 15, 2011, http://www.stratcom.mil/news/2011/220/Lynn_Urges_Partnership_Against_Cyber_Threat (accessed on 18 February 2011).

limited understanding and clarity of the terminology associated with cyber warfare, and lack of clear rules of engagement or clearly developed response actions amplify the weaknesses in the current USG posture on cyberspace.

Who's in Charge? The Need for Strong Centralized Leadership

The 2009 Cyberspace Policy Review (CPR) directed by the Administration identified 24 recommendations, which, when implemented, will improve U.S. capabilities to operate in cyberspace and defend associated infrastructures.² A Government Accounting Office (GAO) assessment released in October 2010 on the progress being made on implementing those recommendations found that only 2 out of 24 recommendations had been fully implemented with minimal progress on the other 22, underscoring the difficulties the USG faces in fully implementing such an approach.³ The GAO study noted that the slow progress was due in large part because agencies had not been assigned specific roles and responsibilities with respect to implementation of the recommendations and that many recommendations were too broad and would take a number of years before being fully implemented.⁴ One of the two recommendations implemented was the naming of national-level cybersecurity coordinator (Schmidt in December 2009) who is supposed to coordinate USG cybersecurity policies and activities. Assignment of specific roles and responsibilities to implement the CPR or other USG initiatives related to cyberspace operations should be designated by the

² See Appendix 1 for a listing of the near- and mid-term recommendations from the Cyberspace Policy Review. GAO, *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed*, (Washington, DC: Government Accounting Office, October 2010), 13.

³ Ibid., 3-4.

⁴ Ibid.

cybersecurity coordinator or his office.

The command and control of overall USG cyberspace efforts is immature at best, and without centralized leadership at the national level, gaps across the various stakeholders will continue, placing USG cyberspace efforts and cybersecurity at risk. Those gaps include planning and synchronization of strategic and organizational activities. DoD takes the lead and coordinates the defense-related initiatives and responses; DHS takes the lead for the rest of the government actions; and private industry coordinates its own responses for protection and operational freedom of its domains. Centralized leadership, with the understanding that the USG can only influence the civil aspects to a limited extent, needs to exist to ensure that those efforts are integrated and synchronized toward a common goal/end-state. Strong leadership will help avoid stove-piped and redundant actions, and encourage a cohesive situational awareness of capabilities and actions. Because of the interdependencies, cyber must have an organization with the authority to direct collective actions, with centralized leadership and decentralized execution.

Deterrence, Dominance or Security: What are We Trying to Achieve?

There are a number of recent U.S. national and military strategies and directives which address, at a high-level, objectives related to security and operations. These documents include the 2010 *National Security Strategy*, the 2010 *Quadrennial Defense Review*, the 2010 *Quadrennial Diplomacy and Development Review*, and the 2011 *National Military Strategy*. Two other governing documents provide more specific guidance: the 2003 *National Strategy to Secure Cyberspace* and the 2006 *National Military Strategy for Cyberspace Operations*. The 2003 *National Strategy to Secure*

Cyberspace identifies three strategic objectives: “prevent cyber attacks against America’s critical infrastructures; reduce the national vulnerability to cyber attacks; and minimize damage and recovery time from cyber attacks that do occur.”⁵ The 2006 *National Military Strategy for Cyberspace Operations* strategic goal is to “ensure U.S. military strategic superiority in cyberspace.”⁶

A lack of a clear cyberspace policy which identifies the overarching strategic cyberspace goals/end-states undermines overall USG efforts. The existing policies fail to establish clearly the nation’s desired end-state and articulate redlines and response actions. A strong national policy will help shape subordinate military, diplomatic and economic efforts, ensuring a unified USG approach to cyberspace operations. An effective cyber deterrent policy should include a strong declaratory policy, build global situational awareness, establish effective command and control across the government, enable strong cyber defense and offensive capabilities, and build on interagency and partner cooperation and collaboration.⁷ A national cyber doctrine can help establish the roles and responsibilities of USG departments and agencies, as well define the relationships with partner organizations and countries.⁸

Developing such a policy is not easy, and a number of experts have drawn parallels between cyber and nuclear weapons use and deterrence. Richard Clarke in his book, *Cyber War*, noted that it took nearly fifteen years after nuclear weapons were first

⁵ *National Strategy to Secure Cyberspace*, iii.

⁶ *National Military Strategy for Cyberspace Operations* (Washington, DC: DoD, December 2006), p.ix. Declassified/FOIA version used. <http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf> (accessed on 21 February 2011).

⁷ Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, eds., *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), 332-336.

⁸ Mark Young, “National Cyber Doctrine: The Missing Link in the Application of American Cyber Power,” *Journal of National Security Law & Policy* [Vol. 4:173], 174.

developed and used before a complex nuclear deterrent and use strategy was developed.⁹ While the *2010 National Security Strategy* indicates that the U.S. will defend our systems, work to develop behavior norms in cyberspace and partner globally to protect the free flow of information and access,¹⁰ it falls short of establishing a declaratory policy articulating possible response actions to cyber attacks. A strong deterrence policy would send a message to state and non-state actors as to the possible ramifications of a cyber attack on U.S. interests.

However, in order to have an effective policy, there will need to be accepted norms and definitions as to what constitutes a cyber attack and thresholds developed which would yield appropriate response actions. Much of what is characterized as “cyber attacks” fall within the realm of cyber espionage (whether for intelligence or economic reasons), or intrusions to determine the vulnerabilities in or to exploit networks, or are criminal in intent. Thresholds will have to be determined based on the results and size of the attack, targets and the identity and intent of the aggressor. Cyber attacks can cause mass disruption, but are unlikely to cause mass destruction (as with nuclear weapons). And of course, a response presupposes that the attack can be attributed accurately to a state/non-state actor. Retaliatory responses to cyber attacks in and of themselves can be problematic. Unlike a nuclear weapons deterrent, where there was no other escalatory weapons in the arsenal, retaliating to a cyber attack risks escalation to other more violent means, including kinetic weapons.¹¹ Martin Libicki points out, because of the asymmetric nature of cyber weapons and war, an attacking state or entity may have nothing worth

⁹ Clarke and Knake, 155.

¹⁰ *National Security Strategy*, 27-28.

¹¹ Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 69.

retaliating against, raising the question of the potential effectiveness of a cyber retaliatory policy in some cases.¹² The USG will have to maintain a number of options in a “retaliatory” toolkit without resorting to a kinetic response. The proportionality of responses needs to be weighed against the effectiveness of kinetic versus non-kinetic attacks against a cyber attacker, who may or may not be impacted by a cyber attack, but where a kinetic attack or application of another instrument of national power (e.g., economic) would be more effective.

Legal Definitions and Attribution? Lessons from the Georgian and Estonian Cases

In order to have an effective whole-of-government approach to responding to cyber threats or actions, there needs to be accepted rules and legal definitions as to what constitutes cyber attacks, cyber warfare or malicious/criminal cyber activity. Defining the nature of the act matters because it helps identify which agency or agencies would be responsible for the detection or response (cybercrime would be handled by national or international law-enforcement agencies according to existing legal conventions, whereas a cyber attack as part of a military action or conflict would logically fall to the military for response actions).¹³ The ability to attribute a cyber attack to an originator will help clarify not only the perpetrator, but also the intent behind the action. The cyber attacks against Estonia and Georgia in 2007 and 2008, respectively, provide examples of the complexities surrounding the definitions and attribution problems.

In August 2008, cyber attacks on Georgia’s internet and communications infrastructure coincided with a Russian military incursion into the country, marking the

¹² Ibid., 70.

¹³ “Cyberwarfare: Marching Off to Cyberwar,” *The Economist*, December 4, 2008, <http://www.economist.com/node/12673385> (accessed on 5 February 2011).

first time identified (and publicized) cyber attacks were used in conjunction with a military conflict. The cyber attacks significantly disrupted Georgia's communications capabilities, disabling a number of web sites, including those serving Georgian government officials, financial institutions and media outlets, for more than a week.¹⁴ The Georgian government accused Russian government of conducting the cyber attacks, although there was no evidence of direct Russian government involvement. A U.S. nonprofit group, U.S. Cyber Consequences Unit (USCCU), assessed that the attacks were caused by Russian criminal groups with no clear linkage to the Russian government, although the timing of the attacks suggests there may have been some Russian government complicity.¹⁵ USCCU further noted that the probable Russian criminal organizations had hijacked U.S. identities and U.S. software tools for use in the attacks on the Georgian websites, controlling some of the attacks via servers in the United States and elsewhere.¹⁶ As a precursor to the August attacks and Russian incursion, as early as mid-July 2008, coordinated distributed denial of service (DDOS) attacks, which can barrage and overload web servers, were being conducted against Georgian servers, successfully shutting down the Georgian President's web site on at least one occasion.¹⁷

The Georgian cyber attacks were a nuisance and a distraction at best, given the limited dependency on the internet by the country at the time. In the spring of 2007, Estonia also came under a barrage of DDOS attacks ostensibly originating from Russia

¹⁴ Siobhan Gorman, "Hackers Stole IDs for Attacks," *Wall Street Journal*, Aug 17, 2009, <http://online.wsj.com/article/SB125046431841935299.html> (accessed on 4 February 2011).

¹⁵ Ibid.

¹⁶ Ibid.

¹⁷ Dancho Danchev, "Georgia President's Web Site Under DDoS Attack from Russian Hackers," ZDNet, July 22, 2008, <http://www.zdnet.com/blog/security/georgia-presidents-web-site-under-ddos-attack-from-russian-hackers/1533> (accessed on 4 February 2011).

following a disagreement over the relocation of a Soviet World War II memorial statue in Tallinn, Estonia. In the case of Estonia, the cyber attacks on that country were more effective because that country is much more reliant on internet technology.¹⁸ The attacks, which lasted for nearly three weeks, blocked websites and nearly shut down the country's Internet infrastructure, significantly disrupting government, banking and communications services.¹⁹

Estonia is a member of NATO and the attacks raises the question as to whether NATO's article 5 (attack on one member state obligates the alliance to attack the aggressor) should be invoked. This comes down to a definition and interpretation of the event: should cyber attacks and/or disruption be considered an "armed attack," an act of war, a crime, or malicious nuisance? As currently defined, the events in Georgia and Estonia would likely not fall under NATO's Article 5. There was no accompanying military action with Estonia, so even if there were clear definitions on cyber attacks and the use of force in cyberspace in NATO's and international laws on war, the Estonian attacks probably would not be characterized as an act of war or an armed attack.

One of the difficulties is attributing the attacks to a particular entity. Is the aggressor in the Estonian and Georgian cases, the Russian government (which has denied involvement in the attacks in either country), an organized crime group, a rogue group, a proxy group, or private citizens? Unlike an attack by traditional weapons, which can be traced to the originator, it can be very difficult to attribute the originator just by following

¹⁸ "Cyberwarfare: Marching Off to Cyberwar."

¹⁹ Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *New York Times*, May 24, 2007, <http://www.nytimes.com/2007/05/29/technology/29estonia.html> (accessed on 5 February 2011).

the path of the “weapon” —the use of remote or intermediate servers often in unsuspecting intermediary countries can obscure the true originator. Whereas military weapons usually are only employed by a military or other identifiable hostile actor (such as a terrorist group), making attribution easier, cyber “weapons” can be readily obtained from internet sites and employed by citizens who rally around a cause (as is suspected in the Estonian case), criminals (as is suspected in the Georgian case), or government entities, or any combination thereof. Difficulties in attributing an attack compound the response actions—should it be a military or law enforcement response, and what should that response be? With respect to the Georgian attacks, NATO’s Cooperative Cyber Defense Center of Excellence in Tallinn, concluded that it was “problematic to apply the Law of Armed Conflict to the Georgian cyber attacks—the objective facts of the case are too vague to meet the necessary criteria of both state involvement and gravity of effect.”²⁰

Laws or rules of war and international agreements will need to be reworked to account for cyber attacks and operations. General Alexander has noted that technology has outpaced policy and law, leaving the USG to deal with telecommunications laws that are from the rotary-dialed phone era.²¹ Policy and legal issues will need to be “brought into the cyber age” if the USG is to leverage all instruments of national power effectively and in a unified manner to ensure freedom of action in cyberspace. Duncan Hollis, a law professor at Temple University, notes that international laws and rules of war do not currently address what constitute “use of force” in cyberspace—leading to problems in

²⁰ Stephen W. Korn, “Botnets Outmaneuvered,” *Armed Forces Journal*, January 2009. <http://www.armedforcesjournal.com/2009/01/3801084/> (accessed on 25 February 2011).

²¹ Jim Garamone, “Cybercom Chief Details Cyberspace Defense,” *American Forces Press Service*, September 23, 2010, http://nispom.us/modules/news/article.php?com_mode=nest&com_order=0&storyid=147 (accessed on January 17, 2011).

interpreting the acts as well as determining response actions.²² Even when the rules and laws are updated or created to reflect the nature of cyber war, there will need to be a framework to determine appropriate response organizations and actions. DoJ will be the lead for establishing and codifying U.S. legal definitions and laws related to cyber. DoD will have to take the lead, nationally as well as internationally, in defining what constitutes cyber war, or an act of war or force in cyberspace, as well as the appropriate response actions to include kinetic and non-kinetic responses.

Partnerships and Authorities: Google and China

Since at least 2003, Chinese-originated cyber attacks and intrusions have targeted Department of Defense, associated defense contracting and other USG computer networks.²³ These attacks were assessed to be part of an organized effort to gain large amounts of information from USG unclassified networks, although there was significant debate as to whether the attacks were part of a Chinese government effort or represented hackers using Chinese servers to obscure the true originators.²⁴ The difficulty in attributing the source of attacks makes it difficult to identify which USG organization is responsible not only for tracking and identifying the activity (intelligence, counter-intelligence, law enforcement, or industry), as well as determining the appropriate response action(s).

Attacks against Google and other U.S. corporations were part of a sophisticated

²² "Cyberwarfare: Marching Off to Cyberwar," *The Economist*, December 4, 2008. <http://www.economist.com/node/12673385> (accessed on 5 February 2011).

²³ Bradley Graham, "Hackers Attack Via Chinese Web Sites: U.S. Agencies' Networks Are Among Targets," *Washington Post*, August 25, 2005, <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html> (accessed on 18 February 2011).

²⁴ Ibid.

espionage effort tracing primarily back to Chinese servers that exploited security flaws in e-mail attachments to access the computer systems of major U.S. financial, defense and technology companies.²⁵ The 2009 attacks on Google targeted e-mail accounts of human rights advocates and organizations in the U.S., China and other countries. If the attacks were perpetrated by a foreign service or government agency, then it would stand to reason that the responsible U.S. agency would be intelligence, defense or law enforcement, depending on the targeted network/host. But if the source of the attacks cannot be determined, should the government be responsible for the detection and defense of a civil network, or should industry? Civil liberties and the authorities under which USG organizations, particularly the Intelligence Community, work restrict the extent to which those capabilities can be employed. This case highlights how current legal and organizational authorities are generally at odds with the borderless and sometimes obscure nature of cyberspace.

NSA, under its foreign intelligence authorities, collects and analyzes foreign threats and activities and provides intelligence derived from its collection and analysis in support of national-level requirement and military operations. Per U.S. law, it cannot and does not target U.S. citizens or corporations to derive intelligence information. Under its information assurance authorities, NSA is able to work with commercial partners in order to identify solutions which protect DoD and national security systems. Since the China-Google attacks represented a vulnerability which could potentially threaten DoD systems, NSA reached an agreement with Google which was designed to allow the two

²⁵ Ariana Eunjung Cha, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say," *Washington Post*, January 14, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html> (accessed on 18 February 2011).

organizations to share critical information to better defend Google from future attacks, without violating Google's policies or laws that protect the privacy of U.S. citizens' communications.²⁶ At the same time, DoD and the USG benefit by gaining information which improves the protection of national security and other USG systems.

Legal authorities and organizational responsibilities need to be clarified and in some cases adapted to the circumstances which require law enforcement, military or intelligence responses to cyber attacks or incidents. The USG also needs to reinforce the authorities which protect civil liberties and privacy while enabling partnership across the military, government and industry to ensure freedom of action and security in the cyber domain.

Information Sharing: “I’ve Got a Secret”

The “WikiLeaks” scenario has had a detrimental effect on sharing of information between USG and international partners. “WikiLeaks” and the resulting restrictions on sharing of information even among USG entities highlights not only the vulnerabilities of secure systems to insider exploitation, it also highlights the fragility and sensitivity of collaborative relationships. These relationships are key to building the trust between organizations which strengthen information sharing policies and processes. Sharing and collaboration, tempered by robust security mechanisms and policies to protect privacy and civil liberties, need to be built into the USG culture and processes.

Information which enables computer network operations is derived from both classified (usually driven by intelligence or law enforcement) and non-classified

²⁶ Ellen Nakishima, “Google to Enlist NSA to Help it Ward Off Cyberattacks,” *Washington Post*, February 4, 2010, <http://www.washingtonpost.com/wpdyn/content/article/2010/02/03/AR2010020304057.html?sid=ST2010020402509> (accessed on 19 February 2011).

(industry) sources. The identity or methods of acquisition of sources from which intelligence is derived often places classification and dissemination restrictions on the information. Classification and dissemination restrictions present barriers to the increasingly rapid (net-speed) provision of information necessary for the development of common operating pictures needed for timely defensive or offensive operations. Policies and processes need to be implemented which facilitate the sanitization and dissemination of critical information to foreign and industry partners while protecting classified source sensitivities, legal disclosure and civil liberties. Blanket sharing policies may be difficult as the threat and operational situations which arise may require unilateral or non-standard approaches between USG and non-USG organizations and multi-national partners. Robust collaboration and information sharing on cyberspace operations must be the standard across all USG departments and agencies, and with the state/local level agencies, commercial/private entities and foreign partners engaged in cyber operations, as appropriate.

One of the key factors to defensive and offensive success in cyber operations will be the ability for the USG, along with industry and foreign partners, to maintain a common operating picture that provides timely and relevant situational threat and operational awareness that can be shared with appropriate government and non-government partners. The common operating picture needs to fully incorporate information and intelligence derived from multiple sources. To enable reactions/actions at “net-speed,” mechanisms need to be in place to enable rapid sharing of threat information with not only military and USG stakeholders, as well with civil authorities and industry. One of the lessons learned from the Cyber Storm exercises (see below) has

been that “early and ongoing information access strengthened the information-sharing relationship between domestic and international cyber response communities.”²⁷ Timely sharing of information is also a critical component of the target vetting and assessment of intelligence gain-loss for cyberspace operations across the Intelligence Community, USCYBERCOM and the supported combatant commands.²⁸

Lessons Learned from the “Cyber Storm” Exercises

Issues related to implementing a whole-of-government approach to work cyberspace issues, at least from a cybersecurity perspective, are best found in the lessons learned from a series of DHS-led cyber exercises. DHS is responsible for conducting a Congressionally-mandated national-level cyber-security exercise series biennially which is designed to strengthen cyber preparedness in the public and private sectors.²⁹ The exercises, known as “Cyber Storm” are the most extensive of USG-sponsored cybersecurity exercises and include federal and state departments and agencies, foreign governments and industry/private sector organizations. There have been three Cyber Storm exercises since their inception in 2006, the most recent being held in November 2010. Given the extent of participation in the exercises, analysis of the lessons learned provides insight into the challenges and issues which a whole-of-government approach engenders.³⁰ (Specific lessons learned from the 2006 and 2008 Cyber Storm exercises can

²⁷ DHS, National Cyber Security Division, *Cyber Storm Exercise Report*, Washington, DC: September 12, 2006, 1-2.

²⁸ “Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command.” <http://armedservices.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf> [accessed on 5 January 2011].

²⁹ DHS Website, “Cyber Storm: Securing Cyberspace,” http://www.dhs.gov/files/training/gc_1204738275985.shtm (accessed on 18 February 2011).

³⁰ Lessons learned are available for the Cyber Storm exercises conducted in 2006 and 2008. Findings from the November 2010 exercise are not available in the public domain as of 18 February 2011.

be found in Appendix 3.)

Common themes in the first two Cyber Storm exercises found weaknesses in interagency coordination and planning; clear articulation of roles and responsibilities; integration of interagency and foreign government relationships (combined operations and vision); correlation and coordination of a common operating picture/situational awareness across multiple organizations; information sharing (particularly beyond the federal level); strategic communications; and commonality of framework and approach. While the results from Cyber Storm III, held in the fall of 2010, are not available, the intent was to build upon the lessons learned in the two previous exercises.³¹

According to DHS, Cyber Storm III was the largest exercise to date, comprising numerous players from seven federal departments, 11 states, 12 partner countries and about 60 companies, designed to exercise the situational awareness and reactions to a large-scale cyber attack on U.S. systems.³² A key objective of the exercise was to test information sharing practices and a new multi-agency center, the National Cybersecurity and Communications Integration Center (NCIC), in its role as an integrating function for DHS and other agencies responding to cyber threats.³³ While initial reports indicate that Cyber Storm III went well, it is likely that some of the challenges and issues which impeded the first two exercises remain.

³¹ "DHS' Cyber Storm III to Test U.S. National Cyber Response Plan," *Homeland Security Newswire*, September 1, 2009, <http://homelandsecuritynewswire.com/dhs-cyber-storm-iii-test-us-national-cyber-response-plan> [accessed on 18 February 2011].

³² Hilton Collins, "Cyber Storm Drill to Yield New Lessons, Feds Say," *Government Technology*, November 5, 2010. <http://www.govtech.com/public-safety/Cyber-Storm-Drill-New-Lessons-Feds.html> (accessed on 18 February 2011).

³³ Shaun Waterman, "Cyber Storm III Aims to Protect Against Real Thing", *Washington Times*, September 28, 2010. <http://www.washingtontimes.com/news/2010/sep/28/cyber-storm-iii-aims-protect-against-real-thing/> (accessed on 18 February 2011).

CHAPTER 4: RECOMMENDATIONS

“One of the things that I think is critical to recognize about cyberspace is that this is beyond the capability of any one government agency to respond or even one government or one private sector entity...this really requires a joint response.”
Philip Reiting, DHS Deputy Under Secretary of National Protection and Programs¹

An effective whole-of-government cyberspace effort needs a concerted and coherent approach to address the strategic challenges and opportunities presented by cyber while mitigating the risks in order to ensure military superiority, securely operate government systems, and protect vital commerce and critical infrastructures.

Technologies and capabilities are rapidly evolving and being deployed in the cyberspace domain, and our adversaries are quickly adopting those changes in order to gain strategic advantages in cyberspace as well as the other domains. If the U.S. is to maintain its leadership in the cyber domain, it needs to have a defined and integrated national cyber framework which allows it to be agile and responsive to the rapidly changing environment. To that end, there are a number of actions which the government, in concert with industry and the private sector, should pursue and implement:

1. Develop a comprehensive national cyberspace policy: The current and past

Administrations have launched a number of programs and initiatives across the USG designed to strengthen and protect the country’s ability to operate in cyberspace. To ensure unity of effort and success of these programs, a coherent national policy needs to be developed and implemented which provides a clear vision and purpose of what

¹ Mickey McCarter, “Cybersecurity Nebraska Ave.: Looking for the Lessons of Cyber Storm III,” *HSToday*, December 1, 2010, <http://www.hstoday.us/focused-topics/cybersecurity/single-article-page/nebraska-ave-looking-for-the-lessons-of-cyber-storm-iii.html> (accessed on 18 February 2011).

the desired U.S. end-states are with respect to cyberspace—is it to secure cyberspace as a means to enable freedom action, deter cyber attacks, achieve dominance, or remain a cyber power? The policy should articulate further in broad terms how the U.S. will shape, defend, and operate within the cyber domain. An overarching national policy will drive specific (and nested) strategies at the department and agency levels which should be designed to meet the goals or end-states identified in the policy. The policy should clearly articulate definitions of cyberspace, cyber attack and cyber warfare, establishing the framework for legal and policy interpretations of cyber operations not only across the USG, but also to establish the associated dialogue in the international community. Given the global nature of the domain, the policy should provide a basis for international engagement and establish a U.S. position on cyber deterrence, making clear the red-lines and ramifications for cyber attacks and warfare to state and non-state actors, a concept that is easier said than done (and implemented/enforced).

2. **Clarify governance for cyberspace issues across the USG:** The current approach to cyberspace operations, and in particular, cyber defense, across the USG and with industry is fragmented. As an adjunct to the policy, the national cyber coordinator through the NSC, should update the existing 2003 National Cyberspace Strategy and implement a new, national cyber strategy which establishes clear lines of authority for planning and executing the cyber mission. That strategy should clearly define the roles, authorities and command and control of the key organizations engaged in cyberspace operations. Leadership should begin with the cyber coordinator, who, as a centralized authority for cyberspace operations, should be empowered to make

decisions and have the authority and resources (i.e., budget) to enforce those decisions. The NSC, in conjunction with the cyber coordinator, should develop U.S. policy initiatives, and be a forcing function to ensure departments and agencies operate effectively toward meeting national security objectives related to cyber issues. Agencies with overlapping authorities must develop effective mechanisms for collaborating on shared activities and work proactively with other stakeholders beyond the USG: state and local governments, industry, private sector, and foreign partners and governments.

As part of addressing governance issues, existing authorities need to be reviewed and updated in order to enable effective partnership and response actions in a timely manner (ideally, at net-speed), while protecting national security capabilities and lines of authority. Standing rules of engagement need to be developed which address various potential scenarios related to cyber attacks to ensure coordination, deconfliction and synchronization of the USG actions. Currently, DoD is responsible for the .mil domain, and DHS is responsible for the .gov domain. The reality of the interdependencies of those domains on each other as well as on the commercial domains means that the division of responsibilities and authorities will be difficult to clearly delineate. Early and close interaction between affected organizations will be necessary to reach a comprehensive understanding of the challenges and solutions to resolving governance issues.

Because much of the government expertise and capabilities for cyber defense lies with the military and given that nearly 90 percent of DoD's networks run through

private domains,² it logically follows those DoD capabilities should be leveraged as appropriate to protect the civil sector, to include critical infrastructure. DoD, in partnership with DHS, should provide leadership to USG cyberspace operations. In some cases, DoD (in particular, USCYBERCOM), given its extensive technical and response capabilities, may need to take sole lead to respond to a threat. To assist DoD in those cases, appropriate authorities and conditions need to be established to enable the DoD to support non-DoD networks.

3. **Create a National-level Cyberspace Operations Center:** It should not take a cyber-equivalent of 9/11 and the resulting legislation and review commissions to create a centralized operations, planning and intelligence activity across the USG. A “National Cyberspace Operations Center” (or similarly named organization) should be established to coordinate and integrate USG efforts while providing current threat awareness, alerts and assessments. Such an organization could be similar to the ODNI’s National Counter-Terrorism Center (NCTC),³ which has both joint strategic planning and joint intelligence functions as part of its charter, and is responsible for synchronizing, planning, and enabling counterterrorism operations across the national, state and local levels and industry, as appropriate. NCTC’s Directorate of Strategic Planning (DSOP) is the nation’s first dedicated, comprehensive government

² Lisa Daniel, “Cyber Solutions Depends on Partnerships, Official Says,” *Armed Forces Press Service*, 8 July 2010. <http://www.defense.gov/news/newsarticle.aspx?id=59942> (accessed on 4 February 2011).

³ NCTC is responsible for joint operational planning *and* joint intelligence, staffed by personnel from the IC, DoD, DoJ, as well as representatives from state, local and tribal agencies. The NCTC has a unique dual line of reporting: (1) to the President regarding Executive branch-wide counterterrorism planning, and (2) to the Director of National Intelligence (DNI) regarding intelligence matters. Its mission includes: “*analyzing the threat, sharing that information with our partners, and integrating all instruments of national power to ensure unity of effort.*” NCTC web site, <http://www.nctc.gov/> (accessed on 4 February 2011).

planning cell for counterterrorism.⁴ Using primarily a military planning model, it has led strategic deliberate planning (the National Implementation Plan for the War on Terror), functional/geographic planning and “near-term dynamic” (crisis) planning across the inter-agency.⁵ The Project on National Security Reform, during a recent evaluation of the organization, noted that DSOP represents one of the most mature interagency teams in the USG today and has the potential to set a precedent for other high-priority, highly complex national missions, such as cybersecurity.⁶

Like NCTC, a national-level cyber center would bring together all elements of national power under centralized leadership to ensure unity of effort. Unity of effort is critical to ensuring cyber power and security of the domain is maintained. A key role for the center would be to lead and coordinate all USG strategic planning for cyberspace operations, along the model of NCTC’s DSOP. The cyber center would also be the lead across the USG for joint intelligence production on cyber threats, and as such, responsible for building, maintaining and sharing a common operating picture, drawn from across the USG and commercial sectors; developing and deploying analytic tools and methods to enable other agencies’ capabilities; and collaborating and sharing information with foreign partners and other stakeholders.

The center would coordinate cyber defense activities and incident responses across the .mil, .gov and .com domains, as well as synchronize and deconflict

⁴ Project on National Security Reform, “Toward Integrating Complex National Missions: Lessons from the National Counterterrorism Center’s Directorate of Strategic Operational Planning,” (Washington, DC: February 2010), xi.

⁵ Project on National Security Reform, “Toward Integrating Complex National Missions: Lessons from the National Counterterrorism Center’s Directorate of Strategic Operational Planning,” (Washington, DC: February 2010), 64.

⁶ Ibid., xviii.

computer network attack operations under the legal authorities of the responsible agencies. One challenge for the center, however, would be to ensure that it is capable of making operational decisions at “net speed”—in hours, if not minutes, and not get caught up in bureaucratic processes which would hinder effective offensive and defensive cyber operations. Additionally, the center should have the authorities necessary to sever and secure specific networks from the overall domains when they are identified as a threat or risk, until which point the threat can be mitigated. While it would be logical to co-locate such a national cyber center with NSA/USCYBERCOM in order to leverage the infrastructure and expertise already located with those organizations, a separate center would help limit the perception of the center being a DoD-centric organization.

4. **Increase international engagement:** The U.S. needs to be the strongest leader in cyberspace issues, and while it may have to work unilaterally to achieve some of its objectives, the global, interconnected nature of cyberspace requires that the U.S. work cooperatively with other countries. The USG needs to work with our foreign partners and international organizations to establish treaties or agreements to establish norms related to behavior and actions in cyberspace, and revise or develop new, international laws and rules of engagement related to cyberspace operations. In effect, the U.S. needs to take the lead in creating a “cyber global community,” which works toward and eventually, enforces, a culture which embraces security and self-regulation which controls cyber crime and warfare. While a cyber “arms control” agreement along the lines of those established in the nuclear and strategic missile realm is likely unachievable, there are multilateral approaches which could be taken

to increase transparency between states on cyberspace operations and to limit cyber warfare. The United States should take a proactive role in developing those approaches in the international community as the immature nature of cyberspace operation presents the ideal opportunity to shape future conditions.

Additionally, the U.S. should make it clear in our policies that punitive actions will be taken against those state and non-state actors who conduct or permit cyber attacks, cyber war, or cyber crime. Given the pervasive nature of anonymity that the internet/cyber domain affords and difficulties of attributing the actual source of an attack or cyber event, the United States will have to establish strong and timely information sharing and collaboration relationships and mechanisms with our partners, as appropriate, in order to identify quickly, malicious actors and activities. Proactive bilateral and multilateral engagements and sharing of situational cyber threat information will protect USG overall national security and economic interests.

Many of the 2011 Mid-East uprisings were facilitated by social media sites and access to the internet or other digital media, resulting in the affected governments censoring or completely shutting down public access. In the wake of those actions, U.S. State Department reiterated its concept of “internet freedom” as a “basic human right” which needs to be protected and secured. Secretary of State Clinton called on foreign governments to eliminate the filtering of internet content and censorship of citizens who use the internet to assemble or provide views.⁷ China, which feels targeted by this policy, has warned the United States not to interfere with its domestic

⁷ “China Faces Internet Dictator's Dilemma: Clinton,” *Reuters*, 15 February 2011, <http://www.reuters.com/article/2011/02/15/us-usa-internet-clinton-idUSTRE71E0P120110215> (accessed on 18 February 2011).

actions and characterized the U.S. position as “cyber hegemony.”⁸ If the USG is to pursue this policy, it will need to be proactive in its diplomatic engagement and strategic communications with those countries, and should build consensus for more widespread support by working through international organizations and alliances such as the UN, NATO, Association of Southeast Asian Nations and the European Union.

5. **Establish effective and integrated planning processes:** Planning efforts associated with cyberspace operations are at best fragmented and mostly stove-piped within the respective departments and agencies, when they are occurring at all. Even the DoD, where USCYBERCOM leads the planning efforts related to cyberspace operations for the military, the newness of the Command and its functions means it is still relatively immature in the development of an overarching cyberspace operations plan and the processes to coordinate and link an overarching plan to service components’ and combatant commands’ plans. Nested under an overarching general cyberspace operations plan, the services and combatant commands should ensure cyberspace operations are included in all deliberate, contingency and crisis plans. Early and continuous inter-agency participation in the development of the cyber component of DoD plans will be critical to ensure the synchronization and integration of efforts.
6. **Build and sustain a capable workforce:** The USG will need a highly trained workforce, a blending of military, civilian and contractor, that is not only technically and operationally competent, but also culturally driven to share information and work jointly. Technical competency can be attained by recruiting highly capable computer

⁸ “Open Source Center Constrained Discussion of “Internet Freedom” in China,” *Public Intelligence*, December 18, 2010, <http://publicintelligence.net/ufouo-open-source-center-constrained-discussion-of-internet-freedom-in-china/> (accessed on 18 February 2011).

scientists, network engineers, and information technology (IT) and security specialists. With the current demand for those specialties, the USG may have to provide incentives (similar the foreign language incentive pay program provided to individuals with critical language skills or college tuition reimbursement/repayment options) to ensure talent is not lost to higher paying jobs in industry. Government-funded programs emphasizing cybersecurity and associated computer skills should continue to emphasize increasing the potential pool of specialists. DoD and DHS have identified the need to increase the cyber-trained workforce and, with NSA, USCYBERCOM and the service cyber components are identifying the core competencies, training and associated recruitment necessary to achieve this goal. The services are adding force structure to the active component elements to address cyber-related shortfalls. All departments and agencies should be taking similar measures to build their cyber workforce.

Joint training and interagency assignments are necessary to drive the culture towards joint operations and sharing, and to raise awareness of interagency and industry cyber operations. The 2010 Intelligence Authorization Act gave the Intelligence Community the authority to detail individuals to DHS or the FBI's National Cyber Investigative Joint Task Force to assist with cybersecurity for a period not to exceed three years, which will help provide needed expertise as well as break down cultural and sharing barriers.⁹ The Pentagon has announced a pilot program that will send high-potential DoD IT employees to industry for up to two years in an

⁹ U.S. Congress, Senate, Report 111-223: Intelligence Authorization Act for Fiscal Year 2010, section 337, http://www.fas.org/irp/congress/2010_rpt/srpt111-223.pdf (accessed on 14 January 2011).

effort to improve the government's IT expertise, particularly in cybersecurity.¹⁰ To build a leadership cadre skilled and informed in cyberspace operations, joint duty assignments to interagency and/or related industry organizations, similar to those required in military and in the IC for advancement to senior levels, should be a mandatory career development and progression milestone for those tracked in cyberspace operations.

7. **Invest in technology and research with industry partners:** In spite of declining government resources, investments need to be made which keep pace with the technological advances in the cyber realm. While this is an expensive venture, not investing in the necessary analytic tools, identity, intrusion detection, security and prevention systems could prove more costly to the country. It is in the military's and broader USG's, as well as industry's interest to collaborate in areas of common concern, primarily in the network defense/security arena, as it is as costly, financially as well as in terms of public support, for industry to suffer a significant cyber breach or attack. Corporations which manufacture and market computer and information technology products (such as Microsoft, Cisco, Intel, and AMD) and the service providers which enable information technology should also be part of the broader USG mechanisms to secure and defend cyberspace. At a minimum, it is in their interests economically to build security features into their products and services, protecting and enabling the government, civil and private capacity to function securely.

¹⁰ Marjorie Censer, "Defense Dept., Private Industry to Trade Workers for A While," *Capital Business*, 3 January 2011, 9.

Government-public consortia should be established to focus on researching, developing and implementing dynamic defensive and enabling technologies. Industry is usually better positioned to provide solutions more quickly which can be adapted to meet USG needs. Deputy Secretary of Defense William Lynn highlighted the need for close DoD and industry partnerships in early February 2011, stating that DoD and other USG organizations should “pursue or expand avenues in information sharing, strengthening network architecture, and extending government's network defenses to private networks key to national security and the economy.”¹¹ In December 2010, the Department of Commerce’s National Institute of Standards and Technology (NIST), DHS’s Science and Technology Directorate, and the Financial Services Sector Coordinating Council (FSSCC) signed an agreement to speed up the commercialization of cybersecurity research innovations to protect government and public critical infrastructures.¹² Increased investment (including budgetary) and partnerships with industry will allow DoD, the USG and industry to be much more anticipatory, rather than reactive, to cyber vulnerabilities and threats.

8. **Learn to manage the risk:** The USG will never be able to deter cyber attacks completely (threats of mutually assured destruction as with nuclear weapons are not effective with cyber attacks given the lack of physical and mortal destruction and often temporary nature of a cyber attack effect). In the near term, and likely for the foreseeable future, the USG will have to establish and maintain an acceptable level of

¹¹ Karen Parrish, “Lynn Urges Partnership Against Cyber Threat,” *Armed Forces Press Service*, 15 February 2011.

¹² White House, Office of Science and Technology Policy, *Partnership for Cybersecurity Innovation*, http://www.whitehouse.gov/blog/2010/12/06/partnership-cybersecurity-innovation?utm_source=related (accessed on 14 January 2011).

risk in its cyberspace operations, focusing limited resources on priority cyber issues and threats. Cyber attacks do not result in the same physical devastation as a kinetic attack; however, given the reliance of governments, economies, critical infrastructures and private citizens on cyber/digital technologies, the disruption of those sectors can have limited, yet significant consequences on a country or society.

One can draw parallels between effectively fighting and preventing cyber attacks and threats and the public health measures used to fight and prevent diseases, or counter a biological weapons threat. While it is unlikely that a disease outbreak can be prevented, the occurrences can be isolated to a limited area or population. An effective public health (or counter-biological threat) campaign includes strong governance in government and private sectors, public awareness, vaccinations and other preventative measures, investment in timely detection research and technology, and rapid and capable response plans and actions to handle outbreaks. If the USG looks at cyber in the same way, then similar response/defense actions can be made. The dynamic nature of cyber means the opportunities, as well as the risk from vulnerabilities, will continue to increase. All USG departments and agencies will need to implement processes and plans which mitigate the risk of operating in cyberspace. Those plans should encompass early detection, warning, active defense operations, public education and awareness, and coordinated response capabilities. Applying similar approaches to public health threats in the cyber field will allow for proactive and timely responses to threats.

CHAPTER 5: CONCLUSION

"From now on, our digital infrastructure -- the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority." President Obama, May 2009 ¹

Dominance in the cyber domain, or perhaps more correctly, the dependency on unfettered access to the capabilities and infrastructure it affords, has become a military and strategic center of gravity for the United States. Freedom of action within and security of the cyber domain is intrinsically tied to national security, economic and social/public interests and well-being. The U.S. military, government, and civilian/societal operations rely heavily on the ability to access and operate freely in cyberspace. The interdependent nature of the cyberspace domain and the capabilities that domain provides means that the solution to dominance or assurance of freedom of action within the domain is not solely the purview of the military or government, but needs to be addressed by a "whole-of-government" and a "whole-of-nation" approach.

The threats to U.S. systems are growing and becoming more complex, particularly as systems and technologies converge. The cyber threat from state and non-state actors will increase, and will likely extend from sources beyond traditional threat states such as Russia, China, and Iran. The advantages provided by a cyber attack (limited investment, anonymity) makes cyber a lucrative asymmetric weapon for states or independent actors. The reliance of a country such as the United States on information technology in virtually every facet of government, defense, business and society increases the state's

¹ Josh Rogin, "Who Runs Cyber Policy?" *Foreign Policy*, February 22, 2010, http://thecable.foreignpolicy.com/posts/2010/02/22/who_runs_cyber_policy (accessed on 25 February 2011).

vulnerability to, and resulting impact of, a cyber attack. Military and government planners can expect any future conflicts to include cyberspace as a critical factor across all operational domains.

State and non-state actors can readily attain the capabilities and tools to exploit vulnerabilities in our weapons, communications and critical infrastructures and systems which rely on digital/cyber technology, a trend which will continue in the foreseeable future. To respond to the threat, the USG needs to respond in an agile and coherent manner, and establish a comprehensive framework which will enable government, industry and foreign partners to work in a coordinated and collaborative manner. There are a number of domestic and international issues that the USG will have to address in order to create an effective response to the challenges posed by cyberspace operations. Any response or framework the USG develops needs to leverage the unique capabilities of the various actors across the diplomatic, information, military, economic, financial, intelligence, and law enforcement spectrum to successfully operate and defend against the threats posed in cyberspace.

The USG has a number of resources at its disposal which can help ensure cyberspace dominance, enhancing our national and economic security. Its greatest strength comes from leveraging the cyber capabilities and resources of the USG Interagency Community, as well as the partnerships developed with industry and allies. To be effective, the USG needs to be proactive in addressing how roles, responsibilities and authorities associated with the cyber mission are divided across departments and agencies and with industry/private sector. It needs to look for better definition, clarity, and efficiencies, and where appropriate, develop more effective governance, policies and

relationships which enable action while protecting privacy and civil liberties. A national cyber strategy should direct and shape the military, government and, as appropriate, industry and private sector, cyber missions to ensure the U.S. has an effective cyber deterrent posture, with robust offensive and defensive cyber capacities which enable it to operate unfettered across a globally-connected domain.

U.S. military security and operations within cyberspace will be enhanced by a comprehensive approach to cyberspace operations. A coordinated and integrated approach to cyberspace operations across USG department and agencies and extending to industry, allies and other partners as appropriate will amplify and strengthen U.S. capabilities to operate within that environment. General Alexander concisely summarized what the USG needs to do to ensure mission success in cyberspace:

Build effective cyber situational awareness capability across all networks, share threat information in a timely manner, synchronize command and control, leverage all tools of national power, conduct international engagement and diplomacy efforts, review military doctrine and actions to ensure they are appropriate and effective, and consider economic and policy tools with intelligence and law enforcement entities to dissuade those who seek to exploit cyberspace for illicit gain.²

To successfully “operationalize” a whole-of-government approach to cyberspace operations, there needs to be a concerted and coherent approach to address the strategic challenges and opportunities presented by cyber while mitigating the risks in order to ensure military superiority, securely operate government systems, and protect vital commerce and critical infrastructures. There is no single capability the U.S can deploy or employ which will guarantee cyberspace dominance; like the domain in which we seek to operate, the solution will have to be interconnected, dynamic and global. Cyber and

²Alexander, “Mission Success in Cyberspace.”

associated information technologies will continue to grow and advance rapidly, as will our reliance on those technologies. The U.S. military alone cannot ensure continued dominance or freedom of operations in cyberspace, whether for its own operations and capabilities dependent on the digital environment, or the greater protection of USG national security systems. Mastering and ensuring freedom of operations in the cyber domain holds the key to the country's national security, economic growth, infrastructure operations and civil functioning. It will take a coherent and comprehensive approach across the USG (and arguably, across the nation and globally) to guarantee superiority and resilience in the cyber domain.

APPENDIX 1: OBAMA ADMINISTRATION’S CYBERSPACE POLICY REVIEW RECOMMENDATIONS

Near- and mid-term recommendations from the May 2009 Cyberspace Policy Review (CPR) follow:¹ (The CPR did not provide a specific timeline for when the near- and mid-term recommendations were to be implemented; the assumption can be made that “near-term” were actions to be accomplished within a year, while “mid-term” within a one-to-three year timeframe.)

Near-Term Actions:

1. Appoint a cybersecurity policy official responsible for coordinating the Nation’s cybersecurity policies and activities; establish a strong NSC directorate, under the direction of the cybersecurity policy official dual-hatted to the NSC and the NEC, to coordinate interagency development of cybersecurity-related strategy and policy.
2. Prepare for the President’s approval an updated national strategy to secure the information and communications infrastructure. This strategy should include continued evaluation of CNCI activities and, where appropriate, build on its successes.
3. Designate cybersecurity as one of the President’s key management priorities and establish performance metrics.
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Convene appropriate interagency mechanisms to conduct interagency-cleared legal analyses of priority cybersecurity-related issues identified during the policy-development process and formulate coherent unified policy guidance that clarifies roles, responsibilities, and the application of agency authorities for cybersecurity-related activities across the Federal government.

¹Unless otherwise noted, recommendations listed are taken verbatim from the *Cyberspace Policy Review*. Office of the U.S. President, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information Communications Infrastructure*, Washington, DC: White House, May 2009, 47- 48.

6. Initiate a national public awareness and education campaign to promote cybersecurity.
7. Develop U.S. Government positions for an international cybersecurity policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cybersecurity.
8. In collaboration with other EOP entities, develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure; provide the research community access to event data to facilitate developing tools, testing theories, and identifying workable solutions.
9. Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation.

Mid-Term Actions:

1. Improve the process for resolution of interagency disagreements regarding interpretations of law and application of policy and authorities for cyber operations.
2. Use the OMB program assessment framework to ensure departments and agencies use performance-based budgeting in pursuing cybersecurity goals.
3. Expand support for key education programs and research and development to ensure the Nation's continued ability to compete in the information age economy.
4. Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.
5. Determine the most efficient and effective mechanisms to obtain strategic warning, maintain situational awareness, and inform incident response capabilities.
6. Develop a set of threat scenarios and metrics that can be used for risk management decisions, recovery planning, and prioritization of R&D.
7. Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.
8. Develop mechanisms for cybersecurity-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial.

- 9.** Develop solutions for emergency communications capabilities during a time of natural disaster, crisis, or conflict while ensuring network neutrality.
- 10.** Expand sharing of information about network incidents and vulnerabilities with key allies and seek bilateral and multilateral arrangements that will improve economic and security interests while protecting civil liberties and privacy rights.
- 11.** Encourage collaboration between academic and industrial laboratories to develop migration paths and incentives for the rapid adoption of research and technology development innovations.
- 12.** Use the infrastructure objectives and the research and development framework to define goals for national and international standards bodies.
- 13.** Implement, for high-value activities (e.g., the Smart Grid), an opt-in array of interoperable identity management systems to build trust for online transactions and to enhance privacy.
- 14.** Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services.

APPENDIX 2: KEY ORGANIZATIONS ENGAGED IN CYBERSPACE OPERATIONS

Organization	Area(s) of Responsibility	Authorities	Key Organizations or Activities	Other
DoD	Operations within and security of .mil domain; commercial networks as associated with Defense Industrial Base or military educational facilities	U.S. Code (USC) Title 10; USC Title 32 (National Guard)	USCYBERCOM	MOA with DHS to provide assistance
USCYBERCOM	Leads DoD offensive and defensive cyber efforts and associated operational, planning, synchronizing activities	USC Title 10	Service cyber elements: 24 th USAF; 10 th Fleet Cyber Command; Army Force Cyber Command; Marine Forces Cyber Command; US Coast Guard Cyber Command (DHS)	Principal DoD component in support of MOA with DHS; can provide assistance to other USG departments on order (and with DHS lead)
DHS	Security of .gov domain; .com/commercial networks associated with critical infrastructure protection. Lead agency for domestic cyber incident response	USC Title 6; HSPD 7; NSPD-54/HSPD-23	US-Computer Emergency Readiness Team; National Cybersecurity and Communications Integrations Center; National Cyber Response Coordination Group	MOA with DoD
DOJ	Criminal activity to include cyber crime; enforcing US laws related to cyber and cyber-related crime.	Multiple U.S. Codes and Laws	Computer Crime and Intellectual Property Section	
FBI	Law enforcement/Protection of U.S. networks from cyber-based attacks and crimes	USC Title 18	National Cyber Investigative Joint Task Force	
DOS	Pursuing freedom of access to internet; diplomatic engagement on cyber issues with states/international organizations		"Coordinator for Cyber Issues"	
Intelligence Community	Provision of intelligence related to state/non-state actors cyber-related activities, to include capabilities, attacks, intrusions, counter-intelligence	USC Title 50	ODNI; CIA; NSA; Joint Interagency Cyber Task Force	
NSA	SIGINT; Information Assurance (IA) for national security systems	USC Title 50 (foreign intelligence); NSD 42 (IA)	National Threat Operations Center	Close relationship with USCYBERCOM; Director is dual-hatted as Cdr, USCYBERCOM
State, Local, Tribal Govts	Cybersecurity of respective networks within jurisdiction		Multi-State Information Sharing and Analysis Center	
Industry	Cybersecurity of respective networks; development of protection software/mitigation of vulnerabilities			
Foreign Partners	Policies and laws related to cybersecurity and operations within countries; establishment of norms related to cyber operations within countries/area of responsibility; cybersecurity of respective networks within jurisdictions.		NATO Cooperative Cyber Defense Center of Excellence (Tallinn, Estonia)	

The following provides additional detailed information not covered in the main text on the specific activities related to cyberspace operations of various organizations across the USG, state, local and commercial entities, and international entities.

DoD: DASD for Cyber Policy

The DASD for Cyber Policy has outlined the following actions and responsibilities which fall under the purview of the office:

- Ensure cyber-related activities are integrated into national and DoD strategies
- Develop, coordinate and oversee implementation of USG and DoD policy and strategy for military and intelligence cyber operations activities.
- Formulates specific DoD policies and guidance related to cyber
- Review and evaluate cyber related programs, plans, and system requirements
- Participate in planning and budgeting activities for space and cyber systems
- Represent OSD at interagency deliberations and international negotiations
- Interface with other USG Departments and Agencies, Congress, the public.¹

USCYBERCOM

USCYBERCOM is a sub-unified command, subordinate to USSTRATCOM. The command has approximately 1,000 military and civilian employees (drawn from existing organizations), and includes a 24/7 Joint Operations Center collocated with NSA that monitors the global information grid, detects attacks and neutralizes the threats. The commander will have both supported and supporting relationships with other combatant commanders, largely identified within the Unified Command Plan, the Joint Strategic Capabilities Plan, execute orders and operation orders.² Five service elements provide support and resources for the command's activities: the Army Forces Cyber Command

¹ DoD Website, "Office of the Deputy Assistant Secretary of Defense for Cyber Policy."

² Alexander, "Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command."

(ARFORCYBER); the 24th USAF; the 10th Fleet Cyber Command (FLTCYBERCOM); the Marine Forces Cyber Command (MARFORCYBER); and the U.S. Coast Guard Cyber Command (CGCYBER).³ With the stand-up of the command, JTF-GNO and JFCC-NW were disestablished and their mission responsibilities and functions absorbed into USCYBERCOM. The command works closely with the service elements to determine specific responsibilities and develop and coordinate offensive and defensive plans and actions. VADM Bernard J. McCullough III, USN, Cdr, FLTCYBERCOM, described the role of the supporting commands to USCYBERCOM as:

using the commonalities between service components to build a network defense-in-depth architecture, allowing our diverse capabilities to create robust and adaptable global cyber defense. If one service discovers, analyzes and defeats a threat, that information can be rapidly disseminated to the other Services to minimize any intrusion effort and create a unified response.⁴

Department of State

In the wake of attacks in Estonia, the Chinese attacks against Google, and most recently, the release of Department of State (DOS) cables on WikiLeaks, the DOS is more aggressively pursuing the role of the diplomatic element of power in cyberspace operations. While U.S. diplomatic engagement on cyber issues has been generally limited, the DOS is taking steps to strategically address the threat and develop a coherent framework to build partnerships with other countries on cyber issues. Secretary of State Clinton has called for unfettered worldwide access to the Internet and has condemned actions by some governments (such as Iran, China, Egypt and other mid-East countries)

³ CGCYBER is a DHS organization.

⁴ House Armed Service Committee, “*Statement of VADM Bernard McCullough III, USN, Before the House Armed Services Committee Subcommittee on Terrorism and Unconventional Threats*,” 111th Cong., 2nd sess., 23 September 2010.

to restrict their citizens' access to the Internet and related communications. According to the Secretary, 21st century statecraft includes “programs that ensure access to the Internet and fight against government censorship.”⁵

The 2010 *Quadrennial Diplomacy and Development Review* (QDDR), released in December 2010, identifies cyber as a global threat, given the dependence of the U.S. on the associated technology and online networks.⁶ The QDDR establishes a new position, “Coordinator for Cyber Issues,” who will lead DOS diplomatic engagement on cybersecurity and other cyber issues, to include the protection and confidentiality of communications between and among governments, a nod to the impact of the leaked cables.⁷ The Coordinator will report directly to the Secretary of State and will serve as liaison to other federal efforts related to cyber issues.⁸

Engagement with foreign countries and the establishment of international laws and norms related to the cyberspace environment is an important aspect of U.S. policy to ensure cyber security and freedom of access to cyber/information technology. A number of cyber experts have called for an “arms control”-like approach to prevent cyber attacks from nations—establishing mechanisms and treaties between the United States and other governments to limit attacks from signatory countries. DOS would be the logical choice to take the lead in cyber arms control negotiations, as it does for nuclear and conventional arms control.

⁵ Tom Krazit and Declan McCullough, “Clinton Unveils U.S. Policy on Internet Freedom,” *CNET News*, 21 January 2010. http://news.cnet.com/8301-30684_3-10438686-265.html (accessed on 14 January 2011).

⁶ *Quadrennial Diplomacy and Development Review*, (Washington, D.C.: Department of State, December 2010), 11.

⁷ *Ibid.*, 7.

⁸ *Ibid.*, 46.

The internet is an important information and diplomatic tool, allowing DOS to promote U.S. programs, values, or counter anti-U.S. messages by various groups. “Public diplomacy 2.0” is the use of the internet and related social media (Twitter, Facebook) as a means to push U.S. strategic communications to reach a broader swath of population (particularly the younger generations) in countries of concern. The flip-side of this capability is the speed, ease and reach which adversaries, or those whose interests may run counter to U.S. objectives, can also use the Internet. As was demonstrated in Tunisia and Egypt, access to the Internet and associated social media enabled the dissenters to publicize rapidly their dissatisfaction and organize their efforts, and the resulting impact, whether intentional or unintentional, had global reach and implications for U.S. national security.⁹ The subsequent Tunisian and Egyptian government responses to the violence was to shutdown access to the Internet or other digital communications, a relatively simple process for states with limited server/network accesses and/or government-owned or -controlled communications. Their actions (of two countries which are considered U.S. allies in the region) and the circumstances under which those actions were taken, highlight the difficulty the U.S. State Department will face in trying to achieve global compliance or standards on government censorship of the Internet or related communications media.

Department of Justice

The Department of Justice (DOJ), under the leadership of the Attorney General, is responsible for enforcing U.S. laws, defending the interest of the United States according

⁹ One could also argue that, as a result of the WikiLeaks disclosure, the content of sensitive DOS cables highlighting actions of government officials acted as an accelerant to enflame civil/popular dissatisfaction and unrest in those countries.

to the law, ensuring public safety foreign and against domestic threats, and providing federal leadership in preventing and controlling crime.¹⁰ Elements of the DOJ, to include the National Security and Criminal Divisions and U.S. Attorneys' offices and the federal Bureau of Investigation (FBI), oversee investigations and prosecution of cyber-related crimes against U.S. persons, institutions and associated networks. DOJ's Computer Crime and Intellectual Property Section (CCIPS) is responsible for implementing the Department's national strategies related to cyber crime and works closely with federal, state and international agencies and the private sector to combat computer and intellectual property crimes worldwide.¹¹

The Federal Bureau of Investigation (FBI)

The FBI is both a federal law enforcement agency (and as such reports to the Attorney General) and a member of the Intelligence Community (reporting to the ODNI). As part of the national security apparatus, the FBI is the lead agency operating domestically to protect and defend the United States against terrorist and foreign intelligence threats, including those that have a cyber nexus.¹² In line with the national security priorities, the FBI identifies one of its top priorities as the protection of the United States against cyber-based attacks and high-technology crimes.¹³

The FBI is lead for the National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF is a Presidentially-mandated activity which brings together various

¹⁰ DOJ public website, "Mission Statement," <http://www.justice.gov/02organizations/about.html> (accessed on 30 January 2011).

¹¹ CCIPS website, "About CCIPS," <http://www.cybercrime.gov/ccips.html> (accessed on 1 February 2011).

¹² *National Cyber Incident Response Plan*, (Washington, D.C.: Department of Homeland Security, 2010), 6.

¹³ FBI public website, "Quick Facts," <http://www.fbi.gov/about-us/quick-facts> (accessed on 1 February 2011).

government agencies, to include intelligence and law enforcement, to coordinate, integrate, and share information related to all domestic cyber threat investigations.¹⁴

Intelligence Community

The Intelligence Community has a diverse set of roles in supporting USG efforts to secure and operate in the cyberspace domain. Human intelligence, signals intelligence and open source intelligence provide indications and warning on cyber attacks to U.S. and foreign networks, information on and assessments of adversary intentions and capabilities, and where possible, attribution of cyber attacks. The NSA, with its vast technical capacity and architecture to monitor foreign cyber and communications activities and provide timely situational awareness, is the primary agency in the Intelligence Community on cyberspace issues.

Office of the Director of National Intelligence

The Intelligence Community (IC), under the auspices of the Office of the Director of National Intelligence (ODNI), oversees the implementation of the classified aspects of the CNCI (with emphasis on those activities associated with the national security systems and the development of a government-wide cyber counterintelligence plan).¹⁵ In further recognition of the need to better synchronize and posture the IC to address cyber issues, the ODNI has established a “National Intelligence Manager for Cyber.” This manager is responsible for the development and implementation of a strategy focused on improving the capacity, integration and synchronization of IC capabilities related to cyber.

¹⁴ FBI public website, “National Cyber Investigative Joint Task Force,” <http://www.fbi.gov/about-us/investigate/cyber/ncijtf> (accessed on 1 February 2011).

¹⁵ House Permanent Select Committee on Intelligence, “*White Paper on Cybersecurity*,” 10 December 2008, 2.

Central Intelligence Agency (CIA)

The Central Intelligence Agency (CIA) is the primary all-source intelligence producer for U.S. policy-makers and the National Human Intelligence (HUMINT) Manager for all IC HUMINT activities. CIA's most recent five-year strategic plan, published in 2010, identified preventing and fighting cyber threats as a key priority. The Agency is investing in human-enabled technical collection and advanced software tools to manage large amounts of data and provide cyber-security monitoring.¹⁶ Issues related to lines of responsibility for offensive cyberspace operations have arisen between DoD and CIA, with the CIA arguing that offensive cyber operations outside a combat zone are covert operations and fall within their purview,¹⁷ although the limits of what constitutes a "cyber combat zone" have yet to be defined. This underscores the need to define the limits and authorities for combat in cyberspace. Oversight for cyberspace operations and clear delineation of related authorities and responsibilities still need to be established and clarified by Administration officials.

Other Federal Departments and Agencies

All Federal Departments and Agencies are responsible for monitoring and ensuring the security of their systems, reporting cyber-related incidents and taking corrective actions as necessary. The Departments and Agencies are required by law to pass information related to cyber attacks, intrusions or security breaches or incidents expeditiously to DHS so a common situational awareness can be maintained.

¹⁶ "CIA Boosting Cybersecurity Investment," *Information Week*, April 27, 2010. <http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=224600617> (Accessed on 30 January 2011).

¹⁷ Ellen Nakashima, "Pentagon is Debating Cyber-Attacks," *Washington Post*, November 6, 2010, 1.

State, Local, Tribal, and Territorial Governments

Under the National Cyber Incident Response Plan, each State, Local, Tribal, or Territorial government is responsible for the cybersecurity of their respective government systems. The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a collaborative state and local government-focused cyber security entity that enables government Chief Information Officers and cybersecurity officials to share threat information and protection capabilities in a timely manner.¹⁸ The MS-ISAC works closely with DHS to analyze and share cyber threat information and implement security practices and capabilities.

Industry/Private Sector

Industry, particularly the information technology sector, through its own monitoring of cyber threats and development of protection capabilities and software is a critical partner to USG governments and agencies. The IT industry has developed special partnerships with the Defense and Homeland Security departments to ensure mutual support on the development and implementation of capabilities to protect both civil and government networks given the interdependencies between the two. Private industry, to include the financial, energy, and transportation sectors, provides information on incidents to DHS primarily through the NCCIC. DOD also provides cyber incident reporting and analysis information to industry partners under the voluntary and collaborative Defense Industrial Base (DIB) Cybersecurity/IA program.¹⁹ Continued

¹⁸ MS-ISAC National Website, “About the MS-ISAC,” <http://www.msisac.org/about/#csac> (accessed on 1 February 2011).

¹⁹ *National Cyber Incident Response Plan*, C-2.

engagement of industry will improve USG capacity to better assess, understand and respond more rapidly to a variety of cyber threats.²⁰

Foreign Partners

Most of the cyber threats to DoD and USG networks originate from outside the United States. Cyber is a shared global capability and any solution or framework the USG develops to guarantee cyberspace operations has to include foreign partners. The U.S. is working both bilaterally and multi-laterally with a number of countries to improve sharing of information, training, and response measures and capabilities related to cybersecurity, although the Cyberspace Policy Review found that the international aspects are among the least developed elements of U.S. policy for cybersecurity.²¹ The 2011 National Military Strategy directs collaboration with international partners, among others, as necessary for the development of “new cyber norms, capabilities, organizations and skills.”²²

The United Kingdom (UK) identified cyber in its 2010 National Security Strategy as a tier 1 threat (on par with terrorism).²³ The UK published a cybersecurity strategy in 2009 and as part of that strategy, created a Cabinet-level Office for Cybersecurity to coordinate policy across government and look at legal and ethical issues as well as relations with other countries. Additionally, a Cybersecurity Operations Center (CSOC)

²⁰ House Armed Service Committee, “Statement of VADM Bernard McCullough III, USN, Before the House Armed Services Committee Subcommittee on Terrorism and Unconventional Threats,” 111th Cong., 2nd sess., 23 September 2010.

²¹ Center for Strategic and International Studies, “Securing Cyberspace for the 44th Presidency. 2008,” http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf (accessed on 31 January 2011).

²² *National Military Strategy 2011*, 10.

²³ “Cyber Attacks and Terrorism Head Threats Facing UK,” *BBC News*, 18 October 2010. <http://www.bbc.co.uk/news/uk-11562969> (accessed on 25 February 2011).

has been established at the Government Communications Headquarters (UK's SIGINT organization) to detect and analyze cyber threats.²⁴

NATO is an active proponent of cybersecurity and related defense issues and is a good example of cooperative international efforts to address cyberspace issues. The 2010 NATO Summit in Lisbon identified cybersecurity as a key security challenge that the organization and its member states will need to address collectively over the coming years. NATO has established a Cyber Defense Management Authority (CDMA) and a Cyber Defense Management Board, which are responsible for establishing policies coordinating cyber defense throughout the Alliance.²⁵ A key issue for NATO will be to address what constitutes, and the threshold for, an “armed attack” (cyber) and what such an attack means in terms of the treaty and response of member states.²⁶

In 2008, in response to the Georgian and Estonian cyber attacks, NATO established a “Cooperative Cyber Defense Center of Excellence” (CCDCOE) in Tallinn, Estonia. The CCDCOE conducts research and training on cyber warfare and includes representatives from 10 NATO countries.²⁷ NATO is accelerating development of a NATO Cyber Incident Response Center in Mons, Belgium, hoping to reach full operational capability by 2012. In November 2010, NATO conducted a cyber defense exercise, with a scenario which included multiple simultaneous cyber attacks targeting NATO and NATO member states. The exercise was to test cyber incident response,

²⁴ “Cyber-Security Strategy Launched,” *BBC On-line*, 25 June 2009, http://news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm (accessed on 5 February 2011).

²⁵ NATO Website, “Defending Against Cyber Attacks,” http://www.nato.int/cps/en/natolive/topics_49193.htm (accessed on 31 January 2011).

²⁶ Kramer, Starr and Wentz, 23.

²⁷ NATO Website, “Defending Against Cyber Attacks,” http://www.nato.int/cps/en/natolive/topics_49193.htm (accessed on 31 January 2011).

interagency collaboration, and the strategic decision making processes of NATO.²⁸ The exercise was deemed a success, with participants exercising their cybersecurity capabilities while collaborating in a multinational incident management environment.²⁹

²⁸ NATO Website, "Cyber Coalition 2010 to Exercise Collaboration in Cyber Defence," http://www.nato.int/cps/en/natolive/news_68205.htm?selectedLocale=en (accessed on 31 January 2011).

²⁹ NATO Website, "Cyber Coalition 2010 Tests NATO's Joint Efforts During Simultaneous Cyber Attacks," http://www.nato.int/cps/en/SID-17D39C37-D508ABA5/natolive/news_69805.htm?selectedLocale=en (accessed on 8 April 2011).

APPENDIX 3: FINDINGS FROM CYBER STORM I (2006) AND II (2008)

Significant findings from the DHS-led national cyber exercise, Cyber Storm I, held in February 2006, included:

- **Finding 1: Interagency Coordination.** While the Interagency Incident Management Group (IIMG) and National Cyber Response Coordination Group (NCRCG) activated and interacted constructively during the exercise, further refinement is needed for operations and coordination procedures. Broader understanding, both within government and in the private sector, of the thresholds and ramifications of activation of these bodies will also improve interagency coordination. Specifically the cyber community needs to better understand the readiness and security postures to be considered based on such activations, as well as the level of Federal engagement they imply.
- **Finding 2: Contingency Planning, Risk Assessment, and Roles and Responsibilities.** Formal contingency planning, risk assessment, and definition of roles and responsibilities across the entire cyber incident response community must continue to be solidified. Responses were timely and well coordinated where existing process procedures were clear and fully understood by players.
- **Finding 3: Correlation of Multiple Incidents between Public and Private Sectors.** Correlation of multiple incidents across multiple infrastructures and between the public and private sectors remains a major challenge. The cyber incident response community was generally effective in addressing single threats/attacks, and to some extent multiple threats/attack. However, most incidents were treated as individual and discrete events. Players were challenged when attempting to develop an integrated situational awareness picture and cohesive impact assessment across sectors and attack vectors.
- **Finding 4: Training and Exercise Program.** An established training and exercise program will strengthen awareness of organizational cyber incident response, roles, policies, and procedures.
- **Finding 5: Coordination Between Entities of Cyber Incidents.** Response coordination became more challenging as the number of cyber events increased, highlighting the importance of cooperation and communication across the community.
- **Finding 6: Common Framework for Response and Information Access.** A synchronized, continuous flow of information available to cyber incident stakeholders created a common framework for response, impact development, and discussions. Early and ongoing information access strengthened the information-

sharing relationship between domestic and international cyber response communities.

- **Finding 7: Strategic Communications and Public Relations Plan.** Public messaging must be an integral part of a collaborated contingency plan and incident response to provide critical information to the response community and empower the public to take appropriate individual protective or response actions consistent with the situation.
- **Finding 8: Improvement of Processes, Tools and Technology.** Improved processes, tools, and training—focused on the analysis and prioritization of physical, economic, and national security impacts of cyber attack scenarios—would enhance the quality, speed, and coordination of response. This is particularly true in the case of integrated or cascading attacks or consequences.¹

Significant findings from the DHS-led national cyber exercise, Cyber Storm II, held in March 2008:

- **Finding 1: Value of Standard Operating Procedures (SOPs) and Established Relationships.** Preparation and effective response is significantly enhanced by established and coordinated SOPs and existing relationships in the cyber response community. These SOPs and relationships facilitate rapid information sharing among community members.
- **Finding 2: Physical and Cyber Interdependencies.** Cyber events have consequences outside the cyber response community, and non-cyber events can impact cyber functionality. Fully understanding this reality is critical to refining comprehensive contingency plans and response capabilities. It is necessary to continue to converge and integrate response procedures tailored for physical crises with those developed for cyber events. The unique activities related to cyber response activities must be highlighted in cyber response processes and procedures to clearly reflect the inherent differences between cyber response and traditional/physical crisis response activities.
- **Finding 3: Importance of Reliable and Tested Crisis Communications Tools.** Tools and related methods developed and deployed for handling crisis communications need further refinement and enhancement. To maximize tools' efficiency and effectiveness during a crisis, the cyber response community needs to examine placement of tools, the impact of tools' capabilities and limitations on

¹ Findings listed are drawn verbatim from the Department of Homeland Security's *Cyber Storm Exercise Report*, 1-2.

response procedures, and identification and authentication protocols used with the tools.

- **Finding 4: Clarification of Roles and Responsibilities.** Substantial improvements since Cyber Storm I were observed in the interagency integration and coordination of cyber event response with senior leadership across interagency boundaries. Continued development and clarification of roles, responsibilities, and communication channels should further enhance our capabilities.
- **Finding 5: Increased Non-Crisis Interaction.** Regular, non-crisis related communications and interaction within the cyber response community through established means would solidify communications paths, strengthen relationships, and clarify organizational cyber incident response roles. Institutionalizing these pathways in non-crisis situations should solidify their role in real world response capabilities.
- **Finding 6: Policies and Procedures Critical to Information Flow.** The maturity and refinement of each organization's policies and procedures correlated directly to the efficiency and effectiveness of information flow between organizations in the exercise. Some key relationships continue to be characterized by one-way communications and unmet expectations.
- **Finding 7: Public Affairs Influence During Large-Scale Cyber Incidents.** An effective and organized public affairs presence has been developed since Cyber Storm I. During a cyber event, public affairs can be used to educate and inform the public through clear, actionable information validated by technical experts and entities such as Sector Coordinating Councils (SCCs) and sector Information Sharing and Analysis Centers (ISACs).
- **Finding 8: Greater Familiarity with Information Sharing Processes.** Cyber response communities understand procedures exist to enable information sharing across classification levels and proprietary boundaries. Exercise findings suggest the value of continued effort devoted to training, use of existing procedures, and familiarity with designation authorities to allow more rapid response and information flow through various mediums.²

² Findings listed are drawn verbatim from the Department of Homeland Security's *Cyber Storm II Exercise Report*. Department of Homeland Security, *Cyber Storm II Final Report* (Washington, DC: July 2009), 3-4.

GLOSSARY¹

Computer Intrusion: An incident of unauthorized access to data or an automated information system.

Computer Intrusion Detection: The process of identifying that a computer intrusion has been attempted, is occurring, or has occurred.

Computer Network Attack (CNA): Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Network Defense (CND): Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.

Computer Network Exploitation (CNE): Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

Computer Network Operations (CNO): Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.

Computer Security (COMPUSEC): The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems.

Critical Infrastructure Protection (CIP): Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include: changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; etc.

Cyber Counterintelligence: Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.

¹ Unless otherwise footnoted, definitions herein are drawn verbatim from the U.S. Department of Defense, *Joint Publication 1-02*, multiple pages.

Cyberspace: A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyberspace Operations: The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

Defense Industrial Base (DIB): The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements

Defense Information Infrastructure — The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving Department of Defense (DOD) local, national, and worldwide information needs. The defense information infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information.

Global Information Grid (GIG): The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems.

Global Information Infrastructure: The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiberoptic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure.

National Information Infrastructure: The nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure.

BIBLIOGRAPHY

- Amoroso, Edward G. *Cyber Attacks: Protecting National Infrastructure*. Burlington, MA: Elsevier Butterworth-Heinemann: 2011. Andruess, Wesley R. "What U.S. Cyber Command Must Do." *Joint Forces Quarterly* 59 (4th quarter 2010): 115-120.
- Alexander, Keith B. "Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command." <http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf> [accessed on 5 January 2011].
- _____. "Cyber Command Posture Statement," 23 September 2010 before the House Committee on Armed Services, 111th Congress, 2nd session.
- _____. "Mission Success in Cyberspace." *Military Information Technology* 14, no. 6 (July 2010). <http://www.military-information-technology.com/mit-home/261-mit-2010-volume-14-issue-6-july.html?layout=default> [accessed on September 12, 2010].
- _____. "Speech Before the Center for Strategic and International Studies on U.S. Cybersecurity Policy and the Role of U.S. Cybercom." http://www.nsa.gov/public_info/files/speeches_testimonies/100603_alexander_trascript.pdf [accessed on 30 January 2011].
- _____. "Statement for the Record Before the House Armed Services Committee Terrorism, Unconventional Threat and Capabilities Subcommittee, 5 May 2009." http://www.nsa.gov/public_info/speeches_testimonies/5may09_dir.shtml [accessed on 31 December 2010].
- _____. "Warfighting in Cyberspace." *Joint Forces Quarterly* 46 (3d quarter 2007): 58-61.
- Bain, Ben. "The Double Edge of the Cyber Sword." *Federal Computer Week*, July 26, 2010, 24-30.
- Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media, Inc., 2010.
- Censer, Marjorie. "Defense Dept., Private Industry To Trade Workers For a While." *Capital Business*, 3 January 2011, 9.
- Center for Strategic and International Studies. "Securing Cyberspace for the 44th Presidency." Washington, DC: CSIS, 2008. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf [accessed on 31 January 2011].

- Cetron, Marvin J., Owen Davies, Stephen Steele, and Cynthia Ayers. "World War 3.0: Ten Critical Trends for Cybersecurity." *The Futurist* 43, no. 5 (October 2009). <http://proquest.umi.com.ezproxy6.ndu.edu/pqdweb?index=1&did=1822785221&SrchMode=1&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1284337872&clientId=3921> [accessed September 12, 2010].
- Chopra, Aneesh and Howard A. Schmidt. "Partnership for Cybersecurity Innovation." The White House Blog, entry posted December 6, 2010. http://www.whitehouse.gov/blog/2010/12/06/partnership-cybersecurity-innovation?utm_source=related [Accessed on 14 January 2011].
- Clarke, Richard A. and Robert K. Knake. *Cyber War: The Next Threat to National Security and What To Do About It*. New York, NY: Harper Collins Publishers, 2010.
- Collins, Hilton. "Cyber Storm Drill to Yield New Lessons, Feds Say." *Government Technology* (November 5, 2010). <http://www.govtech.com/public-safety/Cyber-Storm-Drill-New-Lessons-Feds.html> [accessed on 18 February 2011].
- Corrin, Amber. "Cyber Risks Place New Demands on Public/Private Partnerships." *Federal Computer Week*, July 26, 2010, 32-33.
- Cyber 2020: Asserting Global Leadership in the Cyber Domain*. McLean, VA: Booz Allen Hamilton, 2010.
- "Cyber Strategic Inquiry: Enabling Change Through a Strategic Simulation and Megacommunity Concept." *Summary of Proceedings of Business Executives for National Security*, Booz Allen Hamilton, 2008. <http://www.bens.org/library/publications/CSI'08%20AAR.pdf> [accessed on 25 March 2011].
- Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Washington, DC: The White House, 2009.
- "Cyberwarfare: Marching Off to Cyberwar." *The Economist*, December 4, 2008. <http://www.economist.com/node/12673385/print> [accessed on 5 February 2011].
- "Deputy Secretary of Defense William J. Lynn III on Cyberspace: The U.S. Deputy Secretary of Defense Remarks at the USSTRATCOM and Armed Forces Communications and Electronics Association's 2010 Cyberspace Symposium." *IOSphere* (Spring 2010): 4-9.
- Gibson, William. *Neuromancer*. New York, NY: Ace Books, 1984.

- Grant, Rebecca. *Victory in Cyberspace*. Air Force Association Special Report. Arlington, VA: Air Force Association, October 2007.
<http://www.afa.org/media/reports/victorycyberspace.pdf> [accessed September 10, 2010].
- Hersh, Seymour M. "The Online Threat: Should We Be Worried About a Cyber War?" *The New Yorker*, November 1, 2010: 44.
- Hollis, David M. "USCYBERCOM: The Need for a Combatant Command Versus a Sub-Unified Command." *Joint Forces Quarterly* 58 (3rd quarter 2010): 48-53.
- Hollis, David M. and Katherine Hollis. "Cyberspace Policies We Need." *Armed Forces Journal*, 147, no. 10 (June 2010): 20-24.
- Hoover, J. Nicholas. "Homeland Security, Defense Sign Cybersecurity Pact." *Information Week Government* (October 14, 2010).
<http://www.informationweek.com/news/government/security/showArticle.jhtml?article=227800034> [accessed on 25 February 2011].
- House Armed Services Committee. "*Statement of VADM Bernard McCullough III, USN, Before the House Armed Services Committee Subcommittee on Terrorism and Unconventional Threats.*" 111th Congress., 2nd Session, 23 September 2010.
- Keyes, Charley. "Mullen: Cyber Attack Potential Impact 'Substantial'." *CNN Tech.*, January 12, 2011. http://articles.cnn.com/2011-01-12/tech/cyber.threat_1_cyber-attack-cyber-command-threats?s=PM:TECH [accessed on 15 January 2011].
- Korns, Stephen W. "Botnets Outmaneuvered." *Armed Forces Journal* (January 2009).
<http://www.armedforcesjournal.com/2009/01/3801084/> [accessed on 25 February 2011].
- _____. "Cyber Operations: The New Balance." *Joint Forces Quarterly* 54 (3rd quarter 2009): 97-102.
- Kramer, Franklin D., Stuart H. Starr and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington, DC: National Defense University Press, 2009.
- Kramer, Franklin D. "Cyber Security: An Integrated Governmental Strategy for Progress." *Atlantic Council Issue Brief*. In MiPAL database,
http://www.acus.org/files/publication_pdfs/403/Cyber%20Security%20An%20Integrated%20Governmental%20Strategy%20for%20Progress.pdf [accessed 6 September 2010].
- _____. "Statement Before the House Armed Services Committee Subcommittee on Terrorism and Unconventional Threats." April 1, 2008.

- Krazit, Tom and Declan McCollough. "Clinton Unveils U.S. Policy on Internet Freedom." *CNET News*, 21 January 2010. http://news.cnet.com/8301-30684_3-10438686-265.html [accessed on 14 January 2011].
- Krekel, Bryan. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, prepared for the US-China Economic and Security Review Commission*. McClean, VA: Northrup-Grumman, October 2009.
- Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, DC: Potomac Books, 2009.
- Kueter, Jeff. "Cybersecurity: Challenging Questions with Incomplete Answers." *High Frontier - The Journal for Space and Cyberspace Professionals*, Vol. 6, No. 4 (August 2010): 28-30.
- Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare: China's Master Plan to Destroy America*. Panama City, Panama: Pan American Pub., 2002 (translated version).
- Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York, NY: Cambridge University Press, 2007.
- _____. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.
- Lopez, Jaun Jr. and Dr. Richard A. Raines. "Maximizing the DoD Return on Investment in Cyberspace Professionals." *IAnewsletter* 13, no. 3 (Summer 2010): 16-20.
- Lynn, William, J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (Sep/Oct 2010): 97-109.
- _____. "Mission Assurance in the Face of Cyber Attacks." *High Frontier Journal* 6, no. 4 (August 2010): 24-27.
- _____. "2010 Cyberspace Symposium: Keynote – DoD Perspective." Presented 26 May 2010.
http://www.stratcom.mil/speeches/2010/38/2010_Cyberspace_Symposium_Keynote_-_DoD_Perspective/ [accessed on 8 January 2011].
- McCullough, Bernard, III, VADM. "Statement Before the House Armed Services Committee Subcommittee on Terrorism and Unconventional Threats." 23 September 2010.
- Miller, Robert A. and Daniel T. Kuehl. "Cyberspace and the "First Battle" in 21st-Century War." *Defense Horizons* no. 68 (September 2009): 1-6.

- Moore, Jack. "Cyber Hearings Wrap-Up: Uncertain Road toward Secure Zone." *ExecutiveGov*, September 2010. <http://www.executivegov.com/2010/09/cyber-hearings-wrap-up-uncertain-road-toward-secure-zone/> [accessed on January 16, 2011].
- MS-ISAC National Website. <http://www.msisac.org/webcast/index.cfm> [accessed on 1 February 2011].
- Nakishima, Ellen. "Pentagon is Debating Cyber-Attacks." *Washington Post*, November 6, 2010. 7/
- National Military Strategy for Cyberspace Operations*. Washington, DC: Joint Chiefs of Staff, December 2006. <http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf> [accessed on September 6, 2010].
- National Security Council. "Cybersecurity Progress after President Obama's Address, 14 July 2010." <http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010> [accessed on 13 January 2011].
- National Security Strategy of the United States*. Washington, DC: The White House, 2010.
- National Strategy to Secure Cyberspace*. Washington, DC: The White House, February 2003.
- Nye, Joseph, Jr. *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.
- Nye, Joseph, Jr. *The Future of Power*. New York, NY: PublicAffairs, 2011.
- Office of the Director of National Intelligence. *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence*. Washington, D.C.: ODNI, 2009. <http://intelligence.senate.gov/090212/blair.pdf> [accessed on line 4 January 2011].
- _____. *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence*. Washington, D.C.: ODNI, 2010.
- _____. Statement for the record by the Director of National Intelligence, James R. Clapper. *Worldwide Threat Assessment of the United States Intelligence Community, 2011*. http://www.dni.gov/testimonies/201110210_estimony_hpsci_clapper.pdf (accessed on 15 May 2011).
- _____. National Intelligence Council. *Global Trends: 2025: A Transformed World*. Washington, DC: Government Printing Office, 2008.

- Office of Management and Budget Memorandum. "Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)." Washington, D.C.: Office of Management and Budget, 6 July 2010.
- Office of the U.S. President. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information Communications Infrastructure*. Washington, DC: White House, May 2009.
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [accessed on September 6, 2010].
- Paul, Christopher. *Information Operations Doctrine and Practice: A Reference Handbook*. Westport, CT: Praeger Security International, 2008.
- Project on National Security Reform. *Toward Integrating Complex National Missions: Lessons from the National Counterterrorism Center's Directorate of Strategic Operational Planning*. Washington, DC: PNSR, February 2010.
- Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, MA: The Massachusetts Institute of Technology Press, 2001.
- Redden, Mark E. and Michael P. Hughes. "Defense Planning Paradigms and the Global Commons." *Joint Forces Quarterly* 60 (1st quarter 2011):61-66.
- The Road to Cyberpower: Seizing Opportunity While Managing Risk in the Digital Age*. McLean, VA: Booz Allen Hamilton, 2010.
- Rogin, Josh. "Who Runs Cyber Policy?" *Foreign Policy*, February 22, 2010.
http://thecable.foreignpolicy.com/posts/2010/02/22/who_runs_cyber_policy [accessed on 25 February 2011].
- Rosenback, Eric. "Cyber Security and the Intelligence Community." In *Confrontation or Collaboration? Congress and the Intelligence Community*. Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, July 2009.
http://belfercenter.ksg.harvard.edu/publication/19158/cyber_security_and_the_intelligence_community.html [Accessed on 13 January 2011].
- Rosenzweig, Paul. "10 Conservative Principles for Cybesecurity Policy." *Backgrounders, The Heritage Foundation*, no. 2513 (January 31, 2011).
- Schmidt, Howard. "Cyber Cybersecurity Progress after President Obama's Address, National Security Council." The White House Blog, entry posted July 14, 2010.
<http://www.whitehouse.gov/administration/eop/nsc/cybersecurity/progressreports/july2010> [accessed on 14 January 2011].

- Schmitt, Michael N. and Brian T. O'Donnell, eds. *Computer Network Attack and International Law*. Vol.76 of *International Law Studies*. Newport, RI: Naval War College, 2002
- Sharp, Walter G. *Cyberspace and the Use of Force*. Falls Church, VA: Aegis Research Corporation, 1999.
- Technolytics Institute. *Cyber Commanders' Handbook*. McMurray, PA: Technolytics Institute. 2010.
- Theohary, Catherine A. "Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress." *Congressional Research Service*, September 30, 2009. <http://www.fas.org/sgp/crs/natsec/R40836.pdf> [accessed on 13 January 2011].
- Uda, Robert T., Rhonda Chicone, Bill Shervey, and Darrin Todd. *Cybercrime, Cyberterrorism, and Cyberwarfare: Crime, Terror, and War without Conventional Weapons*. Bloomington, Indiana: Xlibris Corporation, 2009.
- United States Congress. Congressional Cybersecurity Caucus Website. <http://cybercaucus.langevin.house.gov/> [accessed on 14 January 2011].
- _____. House Permanent Select Committee on Intelligence. *White Paper on Cyber Security*. Washington, DC: U.S. Congress, 10 December 2008.
- United States Department of Defense. "Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Forces Command for Military Cyberspace Operations." Washington, D.C.: DoD, 23 June 2009. <http://online.wsj.com/public/resources/documents/OSD05914.pdf> [accessed on 8 January 2011].
- _____. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: Department of Defense, 2001 (as amended through 31 January 2011).
- _____. *Joint Publication 3-13: Electronic Warfare*. Washington, DC: Department of Defense, January 2007.
- _____. "Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity." Washington, D.C.: DoD, 13 October 2010. <http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf> [accessed on 5 January 2011].
- _____. *The National Military Strategy for Cyberspace Operations*. Washington, DC: Department of Defense, 2006. <http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf> [accessed on 21 February 2011]. (Declassified/FOIA version.)

- _____. *The National Military Strategy of the United States of America, 2011*. Washington, DC: Department of Defense, 2011.
- _____. *The Quadrennial Defense Review*. Washington, DC: Department of Defense, 2010.
- _____. Website for the Office of the Deputy Assistant Secretary of Defense for Cyber Policy. <http://policy.defense.gov/gsa/cp/index.aspx> [accessed on 5 January 2011].
- United States Department of Homeland Security. CERT Website. “About Us.” <http://www.us-cert.gov/aboutus.html> [accessed on 14 January 2011].
- _____. CERT Website. “Government Users.” <http://www.us-cert.gov/federal> [accessed on 14 January 2011]
- _____. *Cyber Storm Exercise Report*. Washington, DC: Department of Homeland Security, 2006.
- _____. *Cyber Storm II Exercise: Final Report*. Washington, DC: Department of Homeland Security, 2009. http://www.dhs.gov/xlibrary/assets/csc_ncsd_cyber_stormII_final09.pdf [accessed September 6, 2010].
- _____. “Cyber Storm: Securing Cyberspace.” http://www.dhs.gov/files/training/gc_1204738275985.shtm [accessed on 5 January 2011].
- _____. National Cyber Security Division Website. “National Cyber Security Division.” http://www.dhs.gov/xabout/structure/editorial_0839.shtm [accessed on 14 January 2011].
- _____. *National Cyber Incident Response Plan*. Washington, DC: Department of Homeland Security, 2010.
- _____. “Remarks by Secretary Napolitano at the Atlantic’s Cybersecurity Forum.” 17 December 2010. http://www.dhs.gov/ynews/speeches/sp_1292622750273.shtm [Accessed on 25 February 2011].
- United States Department of Justice. Computer Crime and Intellectual Property Section Website. “About CCIPS.” <http://www.cybercrime.gov/ccips.html>. [accessed on 1 February 2011].
- _____. “Mission Statement.” <http://www.justice.gov/02organizations/about.html> [accessed on 30 January 2011].
- United States Department of State. *Quadrennial Diplomacy and Development Review*. Washington, DC: Department of State, 2010.

United States Federal Bureau of Investigation. “Quick Facts.” <http://www.fbi.gov/about-us/quick-facts> (accessed on 1 February 2011).

United States Government Accountability Office. *Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats*, GAO-10-834T. Washington, DC: General Accounting Office, 2010. <http://www.gao.gov> [accessed September 6, 2010].

_____. *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588. Washington, DC: General Accounting Office, 2008. <http://www.gao.gov> [accessed September 6, 2010].

_____. *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338. Washington, DC: General Accounting Office, 2010.

_____. *Cyberspace Policy: Executive Branch Making Progress Implementing 2009 Policy Review Recommendation, but Sustained Leadership is Needed*, GAO-11-24. Washington, DC: General Accounting Office, 2010.

_____. *Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606. Washington, DC: General Accounting Office, 2010.

_____. *Executive Branch is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed*, GAO-11-24. Washington, DC: General Accounting Office, 2010.

_____. *Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk*, GAO-09-661T. Washington, DC: General Accounting Office, 2009.

_____. *Information Security: Progress made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems*, GAO-10-916. Washington, DC: General Accounting Office, 2010.

United States Joint Forces Command. *The Joint Operating Environment 2010*. Suffolk, VA: Joint Forces Command, 2010.

United States Strategic Command. “US CYBERCOM Fact Sheet.” U.S. STRATCOM, <http://www.stratcom.mil/factsheets/cc/> [accessed on 5 January 2011].

United Nations. *United Nations General Assembly Resolution 3314 (XXIX)*, U.N. GAOR, 6th Commission, 29th Session, December 14, 1974.

- United States Senate. *Senate Report 111-223 – Intelligence Authorization Act for Fiscal Year 2010, section 337*. Washington, DC: United States Congress, 2010.
- Wass de Czege, Huba. "Warfare by Internet: The Logic of Strategic Deterrence, Defense and Attack." *Military Review*, July-August 2010, 85-96.
- Waterman, Shaun. "Internet Traffic was Routed Via Chinese Servers: U.S. Military Sites Included." *Washington Times*, November 16, 2010.
- Wentz, Larry K., Charles L. Barry and Stuart H. Starr, eds. *Military Perspectives on Cyberpower*. Washington, DC: National Defense University Center for Technology and National Security Policy, 2009.
- West, Dondi. "Old vs. New: Legal Considerations of Cyber Targeting." *IO Sphere*, Spring 2010, 10-14.
- Wilson, Clay. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*. CRS Report for Congress. Washington, D.C.: Congressional Research Service, March 20, 2007.
- Wolf, Jim. "Special Report: The Pentagon's New Cyber Warriors." *Reuters.com*. <http://ebird.osd.mil/ebfiles/e20101006779805.html> [accessed on October 6, 2010].
- Young, Mark. "National Cyber Doctrine: The Missing Link in the Application of American Cyber Power." *Journal of National Security Law & Policy* 4: 173.

